Australian Government
Australian Law Reform Commission

Protecting Classified and Security Sensitive Information

DISCUSSION PAPER

You are invited to provide a submission or comment on this Discussion Paper

DISCUSSION PAPER 67
January 2004

ISBN 0-9750600-3-1

Commission Reference: DP 67

The Australian Law Reform Commission was established on 1 January 1975 by the *Law Reform Commission Act 1973* and reconstituted by the *Australian Law Reform Commission Act 1996*. The office of the ALRC is at Level 25, 135 King Street, Sydney NSW 2000, Australia.

Telephone:	within Australia	(02)	8238 6333
	International	+61 2	8238 6333
TTY:		(02)	8238 6379
Facsimile:	within Australia	(02)	8238 6363
	International	+61 2	8238 6363
E-mail:	info@alrc.gov.au		
ALRC homepage:	www.alrc.gov.au		

Printed by The SOS Printing Group (Australia) Pty Ltd

Making a Submission

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 the inquiry.

Submissions are usually written, but there is no set format and they need not be formal documents. Where possible, submissions in electronic format are preferred.

It would be helpful if comments addressed specific questions or numbered paragraphs in this Paper.

Open inquiry policy

In the interests of informed public debate, the ALRC maintains an open inquiry policy. As submissions provide important evidence to each inquiry, it is common for the ALRC to draw upon the contents of submissions and quote from them or refer to them in publications. As part of the open inquiry policy, non-confidential submissions are made available to any person or organisation upon request, and also may be published on the ALRC website.

However, the ALRC also accepts submissions made in confidence. Confidential submissions may include personal experiences where there is a wish to retain privacy, or other sensitive information (such as commercial-in-confidence material). Any request for access to a confidential submission is determined in accordance with the federal *Freedom of Information Act 1982*, which has provisions designed to protect sensitive information given in confidence.

In the absence of a clear indication that a submission is intended to be confidential, the ALRC will treat the submission as non-confidential.

Submissions should be sent to:

The Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001

E-mail: security@alrc.gov.au

The closing date for submissions in response to this DP 67 is 12 March 2004.

Contents

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;[1]
        - section 85B of the *Crimes Act 1914* in relation to in camera proceedings;[2]
        - 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.

1 Section 23V is set out in Appendix 3.
2 Section 85B is set out in Appendix 3.

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:

Division
Professor David Weisbrot
Mr Ian Davis (Commissioner in charge)
Professor Anne Finlay
Mr 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
Jonathan Dobinson

Project Assistant
Alayne Harland

Legal Interns
Adam D'Andretti
Lauren Jamieson
Katherine Jones
Elly Krimotat

Advisory Committee Members

Mr Bill Blick PSM, Inspector-General of Intelligence and Security

Mr Tony Blunn AO, former Secretary of the Attorney-General's Department

The Hon Justice Terry Buddin, Supreme Court of New South Wales

The Hon Justice Tim Carmody, Family Court of Australia

Mr Geoffrey Dabb, former Deputy Secretary of the Attorney-General's Department

Mr Grahame Delaney, First Deputy Director, Office of the Commonwealth Director of Public Prosecutions

The Hon Justice Garry Downes AM, Acting President, Administrative Appeals Tribunal

Mr Des Fagan SC

The Hon John Hannaford QC, former Attorney-General for New South Wales

Mr Tom Howe, Chief Counsel, Litigation, Australian Government Solicitor

The Hon Justice Greg James, Supreme Court of New South Wales

Mr Wayne Martin QC

Professor Garth Nettheim, University of New South Wales

Mr Robert Orr, Deputy General Counsel, Australian Government Solicitor

His Honour Judge Michael Rozenes, Chief Judge, County Court of Victoria

Mr David Sadleir AO, former Director-General of Intelligence

Mr Hadyn Strang, former legal counsel for the Australian Security Intelligence Organisation

Mr Bret Walker SC, New South Wales Bar

Overview

Background

1. Events in recent years have sharply heightened public awareness of matters of national and international security. The role of Australia's security and intelligence agencies—and the control and protection of the critical intelligence information that they generate, share and analyse—is also increasingly a matter of public concern.

2. Cases involving espionage, terrorism and the leaking of national security information have been—and hopefully will remain—quite rare in Australia. However, such cases already have arisen: the successful prosecutions of Australian intelligence officers Simon Lappas (in Australia) and Jean-Philippe Wispelaere (in the United States) for attempting to sell classified national security information are recent examples.

3. Criminal prosecutions highlight these issues most starkly, but problems of principle and practice can arise in a wider array of matters. Classified and security sensitive information is used in administrative decision-making by government officials in circumstances that may give rise to subsequent legal proceedings. For example, such information may be at the heart of a decision to refuse someone the requested security clearance, or to refuse someone a visa, or to revoke a passport, or to resist the production of documents under Freedom of Information laws. Although less common, classified and security sensitive information also may be relevant evidence in a civil lawsuit.

4. The Terms of Reference for this inquiry ask the ALRC to assess the effectiveness of the various existing mechanisms designed to prevent the unnecessary disclosure of classified and security sensitive information in the course of official investigations and criminal or other legal proceedings. The ALRC is also asked to report on whether there are any other approaches, including non-regulatory alternatives, which would improve performance in this area.

5. The protection of national security information will involve many of the same methods already used in the protection of sensitive information or witnesses in criminal prosecutions arising in other contexts—for example, the suppression of the details of undercover operations, and the identity of police informants and undercover agents. The release of such information in open court not only could compromise the effectiveness of police operations, but also risk the lives of these officers and witnesses.

6. There is a very important additional dimension in the need for the protection of classified or sensitive *national security* information, since the risks of disclosure in

these circumstances extend to the very security and defence of the nation, as well as to our strategic interests—not least, Australia's relationships with other nations and our arrangements for the continued exchange of intelligence information.

7. These problems arise most clearly in court proceedings—especially criminal proceedings—where there is a strong common law tradition of 'open justice'. In practice, this means that cases normally are to be conducted in public, and all material evidence will be made available to the parties to examine and test. However, in a matter in which some reliance is, or may be, placed upon classified and security sensitive information, the Government is placed in a quandary. The disclosure of such information may be critical to providing the Crown with sufficient cogent evidence to secure a conviction (or to the Minister for Immigration to justify refusal of a visa, or to a government department to defend an FOI application, and so on).

8. On the other hand, disclosure for these purposes may have very serious consequence outside the courtroom and the logic and needs of the individual case, to the extent of: endangering the lives of intelligence officers; compromising on-going national security operations; revealing hitherto secret information about strategic alliances, techniques, operations, and capabilities; and straining international relationships—whether with allies who have produced or shared information that they do not wish to see made public, or with other nations that learn they are subject of intelligence gathering or unflattering security assessments.

9. In such circumstances, defendants may have an opportunity to employ 'greymail' tactics—the threat to reveal or demand the production of classified or security sensitive information (or a sensitive witness) at trial, with a view to forcing the Government to withdraw or reduce the charges, or enter into a plea bargain (about the severity of the charges or the sentence), on the basis that this unsatisfactory outcome nevertheless ultimately better serves the national interest.

10. The ALRC's challenge is to develop mechanisms capable of reconciling, so far as possible, the tension between disclosure in the interests of fair and effective legal proceedings, and non-disclosure in the interests of national security. It would be an oversimplification, however, to characterise the task as striking a balance between the right of an *individual* to a fair and open trial with the need of the *Government* to maintain official secrets. Due consideration and weight also must be given to the broader and compelling *public* interests in:

- safeguarding national security and strategic interests;
- facilitating the successful prosecution of individuals who engage in acts of terrorism or espionage;

- maintaining the fundamental fairness, integrity and independence of our judicial processes; and

- adhering, to the greatest extent possible, to the principles and practices of both 'open justice' and open and transparent executive government.

Proposed solutions

11. The pattern of Proposals contained in this Discussion Paper seeks to take into account these various interests in a flexible system that incorporates both legal and practical solutions, emphasises the central role of the courts, and is consistent with the Government's stated policies in relation to open government and the proper protection of classified and security sensitive information.

12. In developing these proposals for community consultation, the ALRC has considered the experience in comparable jurisdictions overseas—notably the US, the UK, Canada and New Zealand. For example, all of these countries have specific statutory provisions dealing with the protection and use of classified and security sensitive information—from which we can choose the most effective provisions and strategies.

13. The statutory scheme proposed here would govern the use of classified and security sensitive information in all stages of proceedings in all courts and tribunals in Australia. The ALRC suggests that the scheme be set out in a dedicated new Act—a 'National Security Information Procedures Act'—rather than in the *Evidence Act 1995* (Cth). This should emphasise that the special procedures authorised by the proposed Act are to be used only in a specific category of exceptional cases, outside the general run of law and procedures governing the admission and use of evidence in Australian courts and tribunals.

14. The purposes of the scheme are:

- to identify and bring forward as early in the proceedings as practicable—preferably before the trial—the issues associated with the admission, use and protection of any classified and security sensitive information;

- to provide the court with a wide range of possible methods of maximising the amount of evidence available for use in the proceedings—ensuring that fairness is afforded to all parties (including the Crown) and public access is not unduly restricted; and

- ultimately, to leave the government with the space to make strategic decisions about whether or to proceed, where it considers that (following the court's final rulings on these issues) the risk of disclosure of classified and security sensitive

information in the circumstances outweighs other considerations (such as gaining a conviction or successful defending a civil action).

15. Broadly, the proposed scheme would require all parties to an action to notify the court and the other parties as soon as they learn that any sensitive national security information will arise in the proceedings, whether at trial or in any interlocutory proceedings such as in the discovery of documents. The court must then convene a special directions hearing to determine the way in which this information will be handled during the proceedings. If the Government is not already a party, the Attorney-General of Australia would be notified of the fact that classified or security sensitive information may arise in the proceedings, providing an opportunity to intervene and seek orders governing the protection and use of that information.

16. After hearing all of the arguments in a particular case, the court might rule that the classified and security sensitive information must be admitted into evidence in open court (despite potential adverse consequences for Australia's national security), or that the classified and security sensitive information must be completely excluded (despite the difficulties this may present to the defendant or non-government party).

17. In order to avoid these extremes wherever possible, the ALRC's proposed scheme would give the court a range of options to tailor orders to suit the exigencies of the particular case, including (but not limited to):

- admitting the sensitive material after it has been edited or 'redacted' (the sensitive parts obscured);
- replacing the sensitive material with alternative, less sensitive forms of evidence;
- using closed circuit TV, computer monitors, headphones and other technical means to hide the identity of witnesses or the content of sensitive evidence (in otherwise open proceedings);
- limiting the range of people given access to the sensitive material (for example, limiting access only to those with an appropriate security clearance).
- closing all or part of the proceedings to the public; and
- hearing part of the proceedings in the absence of one of the parties and its legal representatives—although not in criminal prosecutions, and only in other exceptional cases, subject to certain safeguards,

18. In every case, the court would determine admissibility and how the material is to be handled and protected in the proceedings. However, the Attorney-General would

retain the power to certify that the national security information in question is so sensitive that it simply cannot be used under any circumstances. In such a case, the court would retain the final power to determine whether and how the proceedings may proceed in the absence of that material. For example, the court may consider that an accused is placed at such a grave disadvantage that it would be an abuse of process to allow the prosecution to go ahead.

19. In any proceeding in which classified and security sensitive information may be used, the court should have the assistance of a specially trained security officer—as is the case in the United States—to advise on the technical aspects of managing and protecting such information. For example, the security officer would: ensure that the court and the parties are fully informed about the proper handling of such sensitive information; ensure that appropriately secure facilities exist for storing the information when the court is not in session; and facilitate the application and vetting process for any person (such as counsel) who requires a security clearance in order to see the material.

20. The ALRC also makes a number of other Proposals on related matters, including:

- suggested improvements to the structure, content and enforceability of the *Commonwealth Protective Security Manual*;
- methods to monitor the adherence of government agencies to the protective security standards;
- a program for the review of classified material with a view to declassifying it or reducing its classification, and the automatic declassification of classified material that is no longer sensitive after 30 years (subject to any contrary decision taken at that time);
- the restructuring of offences (criminal and administrative) governing the unauthorised disclosure of classified or security sensitive information;
- facilitating the use of injunctions to stop the threatened publication of classified or security sensitive information; and
- the clarification of whistleblowers' protections and procedures for public interest disclosures.

List of Proposals and Questions

Chapter 3 Open Government

Proposal 3–1 The Australian Government should legislate to introduce a comprehensive public interest disclosures scheme. The scheme should cover all Australian Government agencies, including the security and intelligence agencies. The scheme should provide special procedures for dealing with disclosures from and about the intelligence and security agencies and concerning classified and security sensitive information. These procedures should be designed to ensure that classified and security sensitive information is adequately protected and at the same time:

(a) encourage public interest disclosures;

(b) ensure that such disclosures are independently investigated; and

(c) ensure that those making such disclosures are protected from reprisals.

Chapter 4 Commonwealth Protective Security Manual

Proposal 4–1 A revised Australian Government Protective Security Manual should be placed in the public domain, with any sensitive protective security information removed.

Proposal 4–2 Sensitive protective security information that is relevant across the whole of government, or relevant to any particular Australian Government agency, should be included in a separate document or documents. These documents should be classified in accordance with the standards currently set out in the *Commonwealth Protective Security Manual.*

Proposal 4–3 The revised Australian Government Protective Security Manual should be amended to provide further and more explicit guidance about who is authorised to classify information. In particular, it should ensure that information is classified by an experienced officer of appropriately high seniority and holding an appropriately high security clearance.

Proposal 4–4 The minimum standards in the revised Australian Government Protective Security Manual should be amended to include an express statement that: (a) information should only be classified when there is a clear and justifiable need to do

so; and (b) the decision to classify should be based on the criteria set out in the Protective Security Manual and not on any extraneous reason.

Proposal 4–5 The Australian Government should adopt a system of declassifying and reclassifying sensitive material with two elements:

(a) classified and security sensitive information should be reviewed with a view to declassification or reclassification in a number of specified circumstances:

  (i) when it is first classified (which may become unnecessary if Proposal 4–3 is adopted);

  (ii) before transfer to the National Archives of Australia (NAA), in order to reduce the volume of archived material held by the NAA that remains unnecessarily classified;

  (iii) in response to any challenge to its classification status (for example, by recipients of information, as suggested in the *Commonwealth Protective Security Manual*); and

  (iv) when there is any need or proposal to use that information in a public forum such as in court or tribunal proceedings, or in response to a freedom of information application.

(b) automatic declassification 30 years after receipt or creation, to coincide with the period that applies to the release of government papers under the *Archives Act 1983* (Cth), unless a review done at that time concludes that the material should remain classified for a further period of up to five years. These reviews should continue at five-year intervals.

However, classifying agencies should be at liberty to give any item of classified material an earlier date by which the material should be reviewed for reclassification or declassification.

Proposal 4–6 The Australian Government should establish an independent administrative body to review classification decisions, along the lines of the US Interagency Security Classification Appeals Panel.

Proposal 4–7 The Australian Public Service Commission Agency Questionnaire should be expanded to include a section seeking information on agency compliance with protective security standards in relation to the handling of classified and security sensitive information. To the extent appropriate, the results of this section of the Australian Public Service Commission Agency Questionnaire should be included in the annual State of the Service Report to the Prime Minister.

Proposal 4–8 The Inspector-General of Intelligence and Security should seek information on agency compliance with protective security standards in relation to the handling of classified and security sensitive information from the intelligence agencies not subject to the jurisdiction of the Australian Public Service Commissioner. The results should be included in an annual report to the Prime Minister.

Proposal 4–9 The Protective Security Coordination Centre should scrutinise agency responses to the questionnaires and enquiries referred to in Proposals 4–7 and 4–8 with a view to providing agencies with specific advice on improving protective security performance.

Proposal 4–10 Government agencies should be encouraged to schedule internal security auditing procedures so that information collected as part of the internal audit can be used to respond to the annual questionnaires from the Australian Public Service Commission and the Inspector-General of Intelligence and Security.

Proposal 4–11 The Attorney-General's Department should clearly identify, and modify as necessary, those protective security standards in the revised Commonwealth Protective Security Manual intended to be mandatory and enforceable. These standards should then be published in a manner that clearly indicates their mandatory and enforceable nature.

Proposal 4–12 Following the action described in Proposal 4–11, Agency Heads, or other officers with appropriate authority, should direct all staff to comply with those mandatory standards.

Proposal 4–13 To reinforce that direction, agencies should ensure that the standards are well understood and that both new and current employees receive regular training in complying with the standards.

Proposal 4–14 The Australian Government should amend the Australian Public Service Code of Conduct to add a new element stating that Australian Public Service employees are required to comply with the protective security standards described in Proposal 4–11.

Proposal 4–15 The Australian Public Service Commission Agency Questionnaire should be expanded to include a section on agency compliance with the guidelines provided in Part F of the revised Commonwealth Protective Security Manual in relation to contractors who have access to classified and security sensitive information. To the extent appropriate, the results of this section of the Questionnaire should be included in the annual State of the Service Report to the Prime Minister.

Proposal 4–16 The Inspector-General of Intelligence and Security should seek information from the intelligence agencies not subject to the jurisdiction of the Aust-

ralian Public Service Commissioner on agency compliance with the guidelines provided in Part F of the revised Commonwealth Protective Security Manual in relation to contractors who have access to classified and security sensitive information. The results should be included in an annual report to the Prime Minister.

Proposal 4–17 The Protective Security Coordination Centre should scrutinise agency responses to the questionnaires and enquiries referred to in Proposals 4–15 and 4–16 with a view to providing agencies with advice on improving protective security performance by contractors.

Proposal 4–18 Agencies should be encouraged to schedule internal security auditing procedures in relation to contractors so that information collected as part of the internal audit can be used to respond to the annual Australian Public Service Commission and Inspector-General of Intelligence and Security Agency Questionnaires.

Chapter 5 Prevention and Punishment of Unauthorised Disclosure

Proposal 5–1 Sections 70 and 79 of the *Crimes Act 1914* (Cth) and s 91.1 of the *Criminal Code Act 1995* (Cth) should be amended to provide that, where the courts are satisfied that a person has disclosed or is proposing to disclose classified or security sensitive information in contravention of the criminal law, the courts may grant an injunction to restrain such disclosure or further disclosure.

Proposal 5–2 The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information, including in particular regulation 2.1 of the *Public Service Regulations*, to ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.

Proposal 5–3 In conducting the review recommended in Proposal 5–2, the Australian Government should ensure that a clear distinction is drawn between conduct that gives rise to administrative sanctions under the *Public Service Act 1999* (Cth) and conduct that gives rise to criminal sanctions, including those under section 70 of the *Crimes Act 1914* (Cth).

Proposal 5–4 The Australian Government should initiate a comprehensive review of s 79 of the *Crimes Act* to ensure that an appropriate public policy balance is found. Such a review should consider, among other things:

(a) whether criminal liability should require a finding that the unauthorised communication was objectively likely to, or did in fact harm the security or defence of Australia; and

(b) the relationship of s 79 with s 70 of the *Crimes Act* and s 91.1 of the *Criminal Code Act*.

Proposal 5–5 The Australian Government should initiate a review of Commonwealth legislative and regulatory secrecy provisions to ensure that:

(a) each provision is consistent with the Australian Constitution, in particular, the implied freedom of political communication; and

(b) all provisions are broadly consistent, allowing for any necessary variation among agencies.

Chapter 6 Security Clearances

Proposal 6–1 The Legal Aid Guideline requiring lawyers receiving legal aid funding in matters relating to Australia's national security to be security cleared should be rescinded.

Proposal 6–2 There should be no requirement of any sort imposed by the executive government that any judge, magistrate or juror be security cleared before participating in any case.

Chapter 8 Courts—Restricting Disclosure to the Public

Proposal 8–1 As a matter of principle, ministerial certificates should not be conclusive on the question of public interest immunity. Courts should retain a discretion to inspect the material and determine how the information in question should be handled. Governments would retain the ultimate strategic decision-making power in so far as they can withdraw or amend the proceedings to avoid the disclosure of the sensitive material.

Proposal 8–2 Ministers who issue certificates that determine whether information will or will not be disclosed should be required to table in Parliament a notice stating that a certificate was issued, an outline of the circumstances in which it was issued, its effect, and an outline of the process that the Minister went through before issuing the certificate. This would apply in respect of all court proceedings, applications under freedom of information legislation, investigations by the Federal Privacy Commissioner and any other lawful demand for official information that may be denied by a ministerial certificate or similar action.

Question 8–1 Should the Attorney-General issue Legal Services Directions pursuant to the *Judiciary Act 1903* (Cth) in relation to the approach that the Australian Government and its agencies should take in dealing with proceedings involving classified and security sensitive information, including any specific or additional duties which arise in fulfilling the duty to act as a model litigant?

Chapter 10 Proposals for Reform—Courts and Tribunals

Proposal 10–1 The Australian Parliament should enact a National Security Information Procedures Act to deal specifically and solely with the protection of classified and sensitive national security information in court, tribunal and similar proceedings. The procedures to be promulgated by that Act should adhere to the statements of principle set out in the following Proposals.

Proposal 10–2 The Act should cover the use of all classified national security information and other sensitive national security information, whether contained in a document (as defined in the *Evidence Act*) or in oral evidence.

Proposal 10–3 For the purposes of the new Act, 'sensitive national security information' should be defined to include:

(a) 'national security information' as defined in the Commonwealth *Protective Security Manual* that should have been classified but has not been classified; and

(b) other national security information which, if disclosed, might prejudice Australia's defence or security.

Proposal 10–4 The new Act should apply to all stages of proceedings in any Australian court in which classified or sensitive national security information arises.

Proposal 10–5 Each party to proceedings should be required to give notice to the court and to all other parties as soon as practicable after it becomes aware that classified or sensitive national security information is reasonably likely to be used in those proceedings—whether during interlocutory steps (such as discovery, interrogatories and witness statements prepared and exchanged by the parties before any final hearing or trial in the proceedings), at any eventual hearing or trial in the proceedings or in any other way.

Proposal 10–6 The court may of its own motion give the parties in any proceedings the notice referred to in Proposal 10–5.

Proposal 10–7 In civil proceedings or criminal proceedings not conducted by the Commonwealth Director of Public Prosecutions, the court must notify, or direct one or more parties in the proceedings to notify, the Attorney-General of Australia that the notice referred to in Proposal 10–5 or Proposal 10–6 has been given. The Attorney-General of Australia has the right to intervene in the proceedings only in relation to all issues concerning the use of classified or sensitive national security information arising in them.

Proposal 10–8 Once the required notice has been given, the court must hold a directions hearing or similar interlocutory process to determine the future conduct of the proceedings in relation to the use of classified and sensitive national security information. The court may hold such hearings as may be necessary from time to time.

Proposal 10–9 Subject to any orders given by the court, all parties in a proceeding shall file and serve lists of all classified or sensitive national security information that they reasonably anticipate will be used in the proceedings, whether in their own case or in rebuttal to the case of any other party. The court may make such directions as it thinks fit in relation to the specificity with which classified or sensitive national security information is to be described in these lists, the people to whom these lists are to be given, the use that may be made of the information and the degree of protection that must be given.

Proposal 10–10 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may make orders for the further conduct of the proceedings and the use of classified or sensitive national security information, including but not limited to:

(a) Determinations of the relevance and admissibility of any classified or sensitive national security information, including any claims for public interest immunity;

(b) The form in which any classified or sensitive national security information may be tendered to the court as evidence or otherwise used in the proceedings. Such orders may involve:

  (i) the redaction, editing or obscuring of any part of a document containing or adverting to classified or sensitive national security information;

  (ii) replacing the classified or sensitive national security information with summaries, extracts or transcriptions of the evidence that a party seeks to use, or by a statement of facts, whether agreed by the parties or not;

  (iii) replacing the classified or sensitive national security information with evidence to similar effect obtained though unclassified means or sources;

  (iv) concealing the identity of any witness or person identified in, or whose identity might reasonably be inferred from, classified or sensitive national security information or from its use in court (including oral evidence), and concealing the identity of any person (including jurors) who come into contact with classified or sensitive national security information;

  (v) the use of written questions and answers during otherwise oral evidence;

(vi) closed-circuit television, computer monitors, headsets and other technical means in court by which the contents of classified or sensitive national security information may be obscured from the public or other particular people in court;

(vii) restrictions on the people to whom any classified or sensitive national security information may be given or to whom access to that information may be given (which may include limiting access to certain material to people holding security clearances to a specified level);

(viii) restrictions on the extent to which any person who has access to any classified and sensitive national security information may use it; and

(ix) restrictions on the extent to which any person who has access to any classified and sensitive national security information (including any juror) may reproduce or repeat that information.

Proposal 10–11 The court should retain the flexibility to deal with evidence revealing classified or sensitive national security information previously found by the court to be inadmissible or which is raised unexpectedly at the hearing.

Proposal 10–12 Nothing in the proposed new Act should affect the right of a party or the Government to make an application for state interest immunity under s 130 of the *Evidence Act*.

Proposal 10–13 If a party fails to comply with the requirements of the Act or the orders of the court the court may make such orders as its Rules permit including, but not limited to, orders preventing a party tendering or otherwise seeking to use certain material, and from calling or examining certain witnesses, and orders staying, discontinuing, dismissing or striking out that party's case in part or whole.

Proposal 10–14 A party may be excused from non-compliance with the requirements of the Act or the orders of the court if:

(a) the party has good reason;

(b) there is no miscarriage of justice; and

(c) there is no disclosure of classified or sensitive national security information that is not otherwise permitted or authorised by law.

Proposal 10–15 The court should have the power to reduce sentences to take into account the co-operation of the accused with respect to pre-trial disclosure.

Proposal 10–16 In criminal matters, the court may order that the prosecution be excused in part or whole from any obligation that it would otherwise have been under to disclose information to an accused person, or that any such obligation be varied.

Proposal 10–17 On the application of any party or of the Attorney-General of Australia intervening, or on its motion, the court may order that the whole or any part of a proceedings be heard in the absence of:

(a) any one or more specified people; or

(b) the public.

Proposal 10–18 The proposed new Act should include a provision, modelled loosely on s 35(3) of the *Administrative Appeals Tribunal Act 1975* (Cth), to provide that:

(a) in considering an application to close the court to the public or to any party, the court shall take as the basis of its consideration the principle that it is desirable that hearings be held in public and in the presence of all parties;

(b) that evidence given before the court and the contents of documents admitted into evidence should be made available to the public and to the parties, though depending on the nature of the documents the leave of the court may be required to obtain access in accordance with established court rules;

(c) the court should pay due regard to any reason given to it as to why the court should be closed or why the publication or disclosure of the evidence should be prohibited or restricted.

Proposal 10–19 So far as possible, the evidence in support of any application for any order under the new Act should be in open court and, when on affidavit, not sealed.

Proposal 10–20 Written reasons for any order or finding under the new Act should be prepared. The court may then determine to what extent (if at all) those reasons should be sealed, distributed to the public and to the parties or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect classified or sensitive national security information used in proceedings, the court should ensure that any party whose rights are adversely affected by the order receives a copy of the reasons that allows it to pursue any avenue of appeal that may be open to it.

Proposal 10–21 A full transcript of any proceedings heard in the absence of any one or more specified people, the public, any one or more parties, or the legal representatives of any one or more parties should be prepared. The court may determine to what

extent (if at all) that transcript should be sealed or distributed to the public and to the parties or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect classified or sensitive national security information used in proceedings, the court should ensure that all parties receive a copy of the transcript that allows them to pursue any avenue of appeal that may be open to them.

Proposal 10–22 On the application of any party to the proceedings or of the Attorney-General of Australia intervening or any other person, or on its motion, the court may order that any sealed written reasons for any order or any sealed transcript of any proceedings (or any part of them) may be unsealed or published on a wider basis than the court had previously ordered.

Proposal 10–23 The court may require undertakings from any party in the proceedings, their legal representatives, or both, on such terms as the court sees fit, as to the confidentiality and limits on use to be attached to any classified or sensitive national security information. These undertakings may be in addition to, or in substitution for, any other requirement made by the court or the proposed new Act, or sought by any party to the proceedings or the Attorney-General of Australia (including but not limited to any requirement that a party or its legal representatives obtain any security clearance).

Proposal 10–24 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its motion, the court may order that any specified person (including but not limited to any party's legal representatives, court staff, court reporters, expert witnesses or other participant in the proceedings) seek a security clearance to a specified level appropriate to the classified or sensitive national security information used in the proceedings. Alternatively, the court may order that specified material not be disclosed to any person who does not hold a security clearance at a specified level. The court may also make orders about who shall bear the costs of any such clearance.

Proposal 10–25 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its motion, the court may order that the whole or any part of a proceedings be stayed, discontinued, dismissed or struck out if the protection of any classified or sensitive national security information requires that it not be fully disclosed to the court or to a party with the result that any party's rights and ability to fairly and freely present its case and to test the case of, and evidence tendered by, any other party is unfairly diminished.

Proposal 10–26 The court may make such orders as it sees fit in relation to costs and the adjournment of the whole or any part of the proceedings as a result of any requirement of the proposed new Act, order of the court, conduct of the parties or

otherwise in relation to the use of classified or sensitive national security information in any proceedings.

Proposal 10–27 The court may impose such conditions as it sees fit (including the stay, discontinuance, dismissal or striking out of any proceedings in part or whole) on any order that it might make under the proposed new Act.

Proposal 10–28 Either on the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may review any order it makes in relation to the use of classified or sensitive national security information in proceedings. For example, the court may order the disclosure of material that it had previously ordered could be withheld or introduced in another fashion in the light of subsequent developments in the proceedings or elsewhere which alter the requirements of justice in the case or reduce the sensitivity of the material in question.

Proposal 10–29 A court must permit an appeal (if one is sought) from any order requiring any disclosure of any classified or sensitive national security information to be fully determined before any such disclosure is made. Where necessary, a court should grant any leave that might be required by any party in order to pursue any such appeal.

Proposal 10–30 Any other appeals from any order relating to the use of classified or sensitive national security information in proceedings should follow the normal procedures applicable in the court seized of the matter. However, an appeal from any order restricting the access by any party or its legal representatives to any material which is otherwise used in the proceedings and to which other parties have greater access should normally be fully determined before the primary proceedings proceed to final hearing or trial.

Proposal 10–31 Except in the most exceptional circumstances, the law should not permit a statement of any minister, member of the government, statutory office-holder or other government entity to determine the use (or restrictions on the use) of any classified or sensitive national security information in any court proceedings where that determination would, under these principles, have otherwise been made by the court. Any statement by the Attorney-General or other minister or appropriate statutory office-holder would, of course, be given significant weight.

Proposal 10–32 The Attorney-General of Australia or any other person authorised by statute may issue a certificate stipulating that certain classified or sensitive national security information is not to be disclosed to any, or any specified, person in proceedings. The court must then determine whether, in the light of that certificate, the proceedings should be stayed, discontinued, dismissed or struck out in part or whole.

Proposal 10–33 Ministerial certificates about classified and security sensitive information involved in court or tribunal proceedings should be as expansive as circumstances permit in order to allow the court or tribunal to make an informed decision on the appropriate handling of classified and security sensitive information. Where appropriate, such certificates should be accompanied by statements or affidavits from subsidiary decision–makers or other officers briefing the Minister, explaining the decision-making process and, if necessary, why the information that might otherwise seem uncontroversial does in fact have national security implications.

Proposal 10–34 The classification status of a document on its own should never determine any matter under the new Act.

Proposal 10–35 Courts and tribunals should amend their own Rules to the extent necessary to implement the practices and procedures in the proposed new Act, including guidelines in relation to the handling and storage of classified and sensitive national security information.

Proposal 10–36 The relevant Australian Government department or agency should train and assign one or more officers to the federal and other courts, on a permanent basis, to assist the courts in ensuring the protection of any classified or sensitive national security information that is used in proceedings. Such officers would be answerable to the courts to which they assigned and would advise the courts on, apart from other matters, technical aspects of the physical storage and handling of classified or sensitive national security information. However, they would not independently purport to advise the court about the need to protect any material that is not the subject of any court order or ministerial or other certificate.

Proposal 10–37 Section 93.2 of the *Criminal Code Act 1995* (Cth) and s 85B of the *Crimes Act 1914* (Cth) should be repealed.

Proposal 10–38 An accused person and his or her legal representatives should have access to all evidence tendered against him or her.

Proposal 10–39 The taking of evidence involving classified or security sensitive information in civil proceedings before a court or tribunal in the absence of a party whose interests are affected, or the withholding of such evidence received by a court or tribunal from a party in circumstances where the court or tribunal intends to rely on that evidence, should not be permitted where that evidence represents the only or the major piece of evidence against the absent party.

Proposal 10–40 The taking of evidence involving classified or security sensitive information in civil proceedings before a court or tribunal in the absence of a party whose interests are affected, or the withholding of such evidence received by a court or tribunal from a party in circumstances where the court or tribunal intends to rely on

that evidence, should not be permitted except in the most extraordinary circumstances, and then only subject to the following safeguards:

(a) Ministerial certificates should generally not be determinative of the way in which any evidence may be used;

(b) Before consenting to any application that evidence be led in secret, the court or tribunal should consider alternative methods of presenting that evidence such as summaries, stipulations and redactions—which are to be approved by the court or tribunal before use;

(c) The affected person should always be represented by a lawyer, even if that lawyer is not of the person's choosing but a court-appointed lawyer holding any requisite security clearances;

(d) Any tribunal proceedings involving secret evidence should be heard by a judicial member of the tribunal;

(e) There should be an avenue of appeal available to courts on any question of whether the secret evidence should be disclosed to the affected person;

(f) The affected person should always be notified of the fact that secret evidence is being used against him or her;

(g) The normal rules of evidence should apply, including those that involve ex parte hearings; and

(h) A complete record of the whole of the proceedings, including a written statement of reasons for any decision or order made, should be prepared and kept by the court or tribunal. The court or tribunal may determine on a case-by-case basis what (if any) access to the record of proceedings may be permitted.

Proposal 10–41 The fact that a hearing is taking place should never be kept from the party whose rights or interests are being determined or affected by the hearing, whether that hearing is in a court or a tribunal. However, this Proposal is *not* intended to cover hearings in relation to applications for search warrants and applications for approval to adopt other investigative tools.

Proposal 10–42 It should be left to the discretion of the court or tribunal whether there is a need to keep the fact of a hearing secret from the public for a temporary period of time. Permanent suppression from the public of the fact that a hearing has taken place should only be allowed in exceptional circumstances.

PART A

Defining Classified and Security Sensitive Information

1. The ALRC's Inquiry

Contents

Background to the Inquiry

1.1 The Australian Law Reform Commission (ALRC) has been asked to inquire into and report on measures to protect classified and security sensitive information in the course of investigations, legal proceedings, and other relevant contexts. The Terms of Reference are set out in full on pages 5–6 of this Discussion Paper (DP).

1.2 The ALRC is considering whether existing mechanisms adequately protect classified and security sensitive information, or 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 restrictions on the publication of all, or any part, of a proceeding; and the protective security standards set out in the *Commonwealth Protective Security Manual*.[1]

1.3 In assessing these existing mechanisms, the ALRC will have regard to a range of public interests and individual rights that do not necessarily coincide: the rights of individuals to a fair hearing; the general public interest in open government and open court proceedings; and the public interest in the proper pursuit of prosecution of wrongdoers. The ALRC will take into account how Australian and international laws currently protect these interests. The ALRC also will consider proposals to amend Australian law in the light of overseas laws and experience in this area.

1.4 The ALRC's own legislation sets out certain parameters that bind the ALRC in formulating its recommendations. 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 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000). The Manual and the enforceability of the protective security standards it promulgates are discussed in detail in Ch 4.

(a) 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

(b) are, as far as practicable, consistent with the International Covenant on Civil and Political Rights.

1.5 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.[2]

1.6 This inquiry provides all sectors of the Australian community—individuals, civil liberties groups, government agencies, courts, the police and prosecuting authorities, the legal profession, legal aid bodies, the media, and bodies representing migrants and refugees, to name just some—with an opportunity to contribute to developing law and policy in this sensitive area.

1.7 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 doubt that there is some security-related information which, in the national and public interest, should not be disclosed publicly; nor that there are occasions on which the public interests in open justice and open government butt up against a proper need for secrecy. In many respects, this situation is not new and does not arise out of recent events. However, these issues now attract more political and public concern than has been the case previously, and are no longer regarded as isolated and relatively esoteric legal problems.

1.8 It is not the ALRC's task to examine broadly Australia's current or proposed anti-terrorism laws 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. 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 removed.

1.9 The ALRC is currently due to report to the Attorney-General by 29 February 2004. The ALRC published a Background Paper on-line and in CD-rom format on 10 July 2003, and in hard copy from 25 July 2003.[3] Its purpose was to outline the issues raised by the Terms of Reference, to set out the scope of the ALRC's inquiry, and to lay the ground for the ALRC's first round of consultations with, and submissions from, interested parties. Submissions were sought by 29 August 2003, a deadline

---

2 *Australian Law Reform Commission Act 1996* (Cth), s 24(2).

3 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003). It is available at <www.austlii.edu.au/au/other/alrc/publications/bp/8/bp8.html>.

earlier than the ALRC would normally have set, but reflecting the very tight time constraints that the ALRC has been working under in this inquiry. A small number of submissions were received by the deadline, but most were received later, some substantially so. A list of those entities who have made submissions in response to BP 8, or at an earlier stage, is found in Appendix 1 to this DP. The ALRC has had the benefit of a number of meetings with representatives of the security and intelligence agencies in Australia and overseas, but would welcome a formal submission from those agencies in response to this DP to ensure that its final recommendations are based on as complete an understanding of the issues and practices as possible.

1.10 This DP largely supersedes BP 8. Its purpose is to set out the ALRC's preliminary proposals for reform, and acts as the basis for later consultations and submissions focussed on, though not necessarily limited to, those proposals. Although this DP sets out the ALRC's current thinking and possible recommendations, these are by no means settled and the ALRC continues to invite all forms of responses to them and any other matter raised in this Paper. **Submissions in response to this DP are sought by 12 March 2004**.

1.11 Any public contribution to the 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 proposals or numbered paragraphs in this DP. Where possible, submissions in electronic format are preferred.

1.12 In the interests of informed public debate, the ALRC maintains an open inquiry policy. As submissions provide important evidence to each inquiry, it is common for the ALRC to draw upon the contents of submissions and quote from them or refer to them in publications. As part of the open inquiry policy, non-confidential submissions are made available to any person or organisation upon request, and also may be published on the ALRC website. However, the ALRC also accepts submissions made in confidence. Confidential submissions may include personal experiences where there is a wish to retain privacy, or other sensitive information (such as commercial-in-confidence material). Any request for access to a confidential submission is determined in accordance with the *Freedom of Information Act 1982* (Cth), which has provisions designed to protect sensitive information given in confidence. In the absence of a clear indication that a submission is intended to be confidential, the ALRC will treat the submission as non-confidential.

Advisory Committee

1.13 In keeping with its standard practice, the ALRC established an Advisory Committee to assist it in identifying and understanding the issues that emerge from the Terms of Reference, to provide a wide range of experience, to help provide direction to the ALRC's research and consultations, and to act as a sounding board for the ALRC's proposals and, in due course, its recommendations. The ALRC is grateful to all mem-

bers of the Advisory Committee for their continuing support of our work. The names of the members of the Advisory Committee are set out on page 8.

1.14 The ALRC met with the Advisory Committee as a group on 19 September 2003, but has also had the benefit of meetings with a number of its members individually, of notes provided by some of them in response to drafts of various portions of this Paper and the proposals in it, and of other commentary provided informally. The Advisory Committee will meet again before the ALRC finalises its Report.

Structure of Discussion Paper

1.15 The structure of this DP reflects the Terms of Reference, which ask the ALRC to look at the issues surrounding the handling of classified and security sensitive information in two main contexts:

- in a general administrative context (such as in investigations), including a consideration of the enforceability of the security standards set out in the *Commonwealth Protective Security Manual* (PSM); and

- more specifically, the use of classified and security sensitive information in court and tribunal proceedings and similar contexts in which that information might enter the public arena.

1.16 **Part A (Chapters 1 to 3)** of the DP introduces the concept of classifying information, the different categories of classified, security sensitive and other official information, and the consequences that flow when information is classified. This Part also introduces some basic concepts and processes involved with freedom of information, open government and whistleblowers' protection.

1.17 **Part B (Chapters 4 to 6)** considers the handling and protection of classified and security sensitive information in general administrative contexts, and the structure, content and enforceability of the PSM. It also reviews some administrative aspects of security clearance processes.

1.18 As it stands, the PSM is not directly enforceable and attempts to carry out too many functions at the same time—with the result that its effectiveness is compromised. Part B of this Discussion Paper includes a range of proposals that involve re-working the PSM into several documents, each more directed to a specific purpose, with a view to improving the understanding of both basic and detailed information security measures in the general public and within the Australian Government, the Australian Public Service (APS) and among suppliers and contractors to the Australian Government. The ALRC also proposes the revision of some aspects of the APS Code of Conduct and contracts with third parties with a view to making the protective security standards applicable to Australian Government agencies clearly and directly enforceable against members of the APS and third party contractors.

1.19 Thus far, there has been no submission to the ALRC asserting that the standards within the PSM are themselves inadequate; however, there is some evidence that they are not universally observed. The ALRC's proposals consider some methods of improving compliance with existing security standards and involve a more structured approach to the initial classification of sensitive material; time limits on classification; the review of classification decisions; and the imposition of penalties for the use of classification procedures for improper purposes.

1.20 **Part C (Chapters 7 to 10)** reviews the principles of fair trials; the methods currently used in Australian and overseas courts and tribunals to determine whether to restrict access to classified or security sensitive information to the public, to a party to the proceedings or to any person whose interests are affected by them; the techniques used to put these principles into practice; and other such techniques that might be applied in Australia.

1.21 Chapter 10 sets out a comprehensive set of proposals for the enactment of new measures that represent a consolidation of the procedures that are, or should be, adopted in Australian courts and tribunals and in other official inquiries. These procedures seek to balance the need to keep certain classified and security sensitive information secret with the public interest in open government and open and fair justice. In short, they require parties to proceedings in which classified or security sensitive information is likely to arise to inform the court and the other parties accordingly once they become aware of this possibility. The Attorney-General is to be notified if an appropriate Australian Government agency is not otherwise party to or aware of the proceedings. The new procedures permit the parties (or the Attorney-General intervening) to apply to the court well in advance of any trial or final hearing in the case to seek to exclude certain material, to replace it with an alternative form of admissible evidence, and to adopt various techniques in court to protect sensitive information while still permitting the greatest public access to all proceedings appropriate to the case in question.

1.22 In all cases, the court's paramount concern is the interests of justice in the case before it. The Government, through the Attorney-General, retains a final right to refuse to permit certain information to be used in proceedings in order to protect the security or defence of the Commonwealth. The court, however, retains the power to determine how, if at all, the case should proceed in the light of any such refusal.

1.23 A summary list of the proposals contained in this DP may be found immediately preceding this Chapter, starting at page 15.

1.24 There are four appendices to this DP:

Appendix 1: a list of the individuals and entities who have provided written submissions to the ALRC in response to BP 8;

Appendix 2: a list of abbreviations and acronyms found in this DP;

Appendix 3: a selection of extracts from statutes and international instruments referred to in the Terms of Reference and recurrently in this DP; and

Appendix 4: a summary of the proceedings in *R v Lappas and Dowling* (so far as can be discerned from the limited amount of material published from that case)—since this case appears to have been a critical element in the Australian Government's decision to issue the Terms of Reference in this inquiry and because it is the only major espionage trial in Australian jurisprudence.[4]

4 The only two published judgments in this case are the trial judge's Reasons for Ruling on the prosecution's claim for state interest immunity in *R v Lappas and Dowling* [2001] ACTSC 115 and the judgment of the Court of Appeal of the Australian Capital Territory on the Crown's appeal against sentence in *R v Lappas* [2003] ACTCA 21. The summary that appears in Appendix 4 incorporates material from other published materials, in particular newspaper reports.

2. Classifying Information

Contents

What is classified information?

2.1 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.

2.2 The PSM uses the terms 'national security information' and 'non-national security information' to refer to information requiring classification. It notes that, in the past, national security information was often referred to as 'classified', while non-national security information was known as 'sensitive'.[1] This caused confusion as both types of information could be subject to a classification process.

2.3 Once information is classified, it is marked accordingly and given various forms of protection—including restricting access to people with a security clearance at the appropriate level; physical protection, such as storage in approved containers of sufficient strength or meeting other security standards; and restrictions on how it may be transferred from one person to another. However, the fact that information is *not* classified does not mean that it is freely available. For example, the *Privacy Act 1988* (Cth) and similar laws restrict the dissemination and use of certain personal information. All official information (ie, information developed, received or collected by or on behalf of the government):

1 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 29, [6.21]. The definitions of these terms are discussed in more detail below.

- 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.[2]

2.4 As a general matter, government officers are only entitled to information that they have a need to know to carry out their functions properly.[3] However, certain legislation—most notably the *Freedom of Information Act 1982* (Cth)—gives the public rights of access to government-held or government-controlled information, subject to a number of exceptions and exemptions, one of which is national defence and national security.[4]

2.5 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.[5]

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

2.7 The PSM distinguishes between national security information and non-national security information. It defines **national security information** as:

> any official resource (including equipment) that records information about or is 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 relates to significant political and economic relations with international organisations and foreign governments

---

2 Ibid, C 5, [1.3]. The second of these points is a statement of the 'need to know' principle.
3 Ibid, C 9, [2.4].
4 Although this may be expressed in a variety of ways. See Ch 3.
5 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 6, [1.4]. It is worth noting the distinction drawn between public interest and government interest: there might be occasions when the two do not coincide.

- **national interest**, that relates to economic, scientific or technological matters vital to Australia's stability and integrity.[6]

2.8 National security information may be given one of four national protective security markings based on an assessment of the consequences of the unauthorised disclosure of the information:

- 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.[7]

2.9 The PSM stresses that government policy is to keep classified information to a minimum. The mere fact that information relates to national security is not sufficient to *require* classification—that becomes necessary only if unauthorised disclosure of the information could cause damage to national security.[8] The PSM notes that most national security information requiring classification will be adequately protected by the procedures established for dealing with Restricted and Confidential material. It recommends that the Secret marking be used sparingly and the Top Secret marking with the 'utmost restraint'.[9]

2.10 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. 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

6 Ibid, C 29, [6.22].
7 Ibid, C 31, [6.29]–[6.34].
8 Ibid, C 29, [6.23]–[6.25].
9 Ibid, C 31–32, [6.32]–[6.34].

- **personal information** that is required to be protected under the provisions of the Privacy Act, the Archives Act, or other legislation.[10]

2.11 Where necessary, 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: see [2.13] below);

- 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.[11]

2.12 The PSM notes that most non-national security information requiring classification will be adequately protected by the procedures established for dealing with the first two of these markings, and that 'Highly Protected' should be used 'sparingly'.[12]

Cabinet documents

2.13 Documents prepared for use by Cabinet to formulate policy and make decisions are given special protection on the basis that unauthorised disclosure would damage the fullness and frankness of discussions in the Cabinet Room and would thereby inhibit the process of good government. These documents are marked Cabinet-in-Confidence regardless of any other security consideration. The *Cabinet Handbook* stipulates that Cabinet-in-Confidence documents require a level of protection at least equivalent to that given to documents classified as Protected under the guidelines set out in the PSM.[13]

Foreign-sourced documents

2.14 Information received by Australian government agencies from another country 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.[14] Australia has entered into bilateral treaties with a number of countries, including the United

10 Ibid, C 30, [6.24].
11 Ibid, C 32, [6.35]–[6.42].
12 Ibid, C 33–34, [6.41]–[6.43].
13 Department of the Prime Minister and Cabinet, *Cabinet Handbook* (5th ed, 2002), 28, [7.5].
14 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 27, [6.12].

States of America,[15] concerning security measures for the protection of classified information received from those other countries. The agreement with the US requires that Australia not use, or permit the use of, classified information received from the US for any other purpose than that for which it was provided without the prior written approval of the US.[16] It has been emphasised to the ALRC that classified and security sensitive information must be protected to ensure that vital channels of intelligence of national importance remain open to Australian defence and intelligence agencies.[17]

2.15 The Terms of Reference do not expressly limit the ALRC's consideration of classified information to national security information, but that is clearly the focus of current public debate and the major prompt for the Australian Government to refer these issues to the ALRC. For this reason, the Proposals in this DP are expressed to apply to national security information. In developing these Proposals, however, the ALRC has also examined existing mechanisms for dealing with non-national security information in courts and tribunals. The ALRC's proposals in relation to national security information may also have some application to other classes of information (such as classified information generally).

What is security sensitive information?

2.16 While it is relatively straightforward to identify classified information, the ALRC has also been asked to consider the protection of 'security sensitive information'. 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.'

2.17 In its submission, the Attorney-General's Department clarified that:

> The term 'security sensitive information' was **not** intended to refer to information that is not of sufficient importance to damage national security interests. The term was intended to refer to national security information that should have been, but was not, security classified.[18]

2.18 On this basis, security sensitive information would seem to include only information that is classifiable and falls into two relatively narrow categories:

(a) information worthy of being classified that simply has not yet been classified in that small window of time falling between its receipt or creation by the relevant agency and the agency actually performing the administrative task of classification; and

---

15 *Agreement between the Government of Australia and the Government of the United States of America Concerning Security Measures for the Protection of Classified Information*, 25 June 2002, Australia and United States of America, [2002] ATS 25, (entered into force on 7 November 2002).

16 Ibid, Art 4C.

17 D Sadleir, *Consultation*, Sydney, 3 December 2003; Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

18 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

(b) information worthy of being classified but which, whether by error or oversight, has not been classified.

2.19 The ALRC's consultations and submissions suggest that it is the substance of the material under consideration, and not its security marking (if any), that is paramount in any given context. This does not mean that the failure to give sensitive material a security marking, or the decision not to give it a marking or to give it a particular marking, is not important. However, it has become clear that, when considering the use of sensitive material in court or tribunal proceedings, a marking ought to be no more than one factor to be taken into account, albeit a significant one.

National security information

2.20 It is important to distinguish the information that is at the heart of this inquiry from other sensitive information that 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 victims or 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.

2.21 In many respects, the classified and security sensitive information that is central to this inquiry includes material of this sort. However, it also includes:

- information concerned with Australia's national security, defence, international relations and other important strategic interests;
- information, the mere existence of which is sensitive as it would reveal the existence of relationships or covert operations that could compromise Australian or allied interests;[19] 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, the disclosure of which would also endanger the further exchange of security information.

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

---

19 In these cases, the relevant government agency would wish to neither confirm nor deny that the information exists. This may be so even if the information were available from non-classified sources as the mere fact that it has been obtained by the agency could hint at the existence of certain intelligence operations.

- identifying to foreign powers and others the capabilities (or limitations) of Australia's intelligence services and defence arrangements;
- undermining international or diplomatic relations; and
- confirming the existence of matters which could otherwise only be the subject of public speculation.

2.23 However, the methods by which confidential operational law enforcement information is handled by Australian courts—which is an every-day occurrence—provide a useful point of comparison when considering how national security sensitive material might be handled in court and tribunal proceedings. Australian courts, tribunals and lawyers are very experienced at handling sensitive and confidential information of many sorts, and the techniques that have been developed to meet these problems may offer guidance on protecting and using classified and security sensitive information in public courts and tribunals.

Security and intelligence agencies

Australian agencies

2.24 The Australian Security Intelligence Organisation (ASIO) is Australia's domestic intelligence agency. It is responsible for gathering information and intelligence to make security assessments and to advise government about risks to national security. ASIO also provides protective security advice to government agencies and assessments of individuals seeking national security clearances or visas to enter or stay in Australia.[20] ASIO falls within the portfolio responsibilities of the Attorney-General. 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'.[21]

2.25 The *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Cth) significantly expanded ASIO's powers to include certain 'police powers' in relation to terrorism offences. The Act provides that the Director-General of ASIO may seek a warrant to detain and question individuals in relation to such offences.[22]

2.26 The Australian Secret Intelligence Service (ASIS) collects overseas intelligence about the capabilities, intentions and activities of people or organisations outside Australia that may impact on Australian interests and security. ASIS also conducts counter-intelligence activities and liaises with foreign intelligence and security agencies. ASIS

---

20 Australian Security Intelligence Organisation, *Australian Security Intelligence Organisation Home Page*, <www.asio.gov.au/> at 28 August 2003.

21 *Australian Security Intelligence Organisation Act 1979* (Cth), s 4.

22 See the discussion of ASIO's powers of detention and interrogation in Ch 8.

falls within the portfolio responsibilities of the Minister for Foreign Affairs.[23] The *Intelligence Services Act 2001* (Cth) formally establishes and sets out the functions of ASIS. There are a number of express limits on the activities that ASIS can undertake; for example, the Act provides that ASIS is *not* a police or law enforcement agency and must not plan for, or undertake, paramilitary activities or activities involving violence against the person or the use of weapons.[24]

2.27 On 15 October 2003, the Government introduced the Intelligence Services Amendment Bill 2003 into Parliament. If passed in its current form, the Bill will amend the *Intelligence Services Act* in a number of ways, including: to allow ASIS officers and agents to cooperate with other organisations in planning and undertaking paramilitary activities, activities involving violence against the person, or the use of weapons so long as ASIS itself does not undertake those activities. The Bill would also allow ASIS officers and agents to carry weapons for the purposes of self-defence.

2.28 The Defence Intelligence Group in the Department of Defence comprises three units: the Defence Signals Directorate (DSD), the Defence Intelligence Organisation (DIO) and the Defence Imagery and Geospatial Organisation (DIGO). All three bodies fall within the portfolio responsibilities of the Minister for Defence.

2.29 The *Intelligence Services Act* sets out the functions, and certain limits on the activities, of the DSD. The DSD has the task of obtaining intelligence about the capabilities, intentions or activities of people or organisations outside Australia through the collection of foreign signals intelligence. It also provides advice to the Australian Government on the security and integrity of information kept in electronic form and other information technology issues.[25]

2.30 The DIO provides intelligence assessments based on information from a range of sources to support the Department of Defence, the planning and conduct of defence force operations and wider government decision making. The DIO's assessments focus mainly on the Asia-Pacific region.[26]

2.31 The DIGO extracts intelligence information from imagery and other sources, such as photographs and digital images collected by satellites and unmanned airplanes. The DIGO uses these resources to locate and assess physical features, observable phenomena and activity that may affect Australia's interests.[27]

---

23 Australian Secret Intelligence Service, *The Australian Secret Intelligence Service*, <www.asis.gov.au/asiscorpinfo.html> at 29 May 2003.

24 *Intelligence Services Act 2001* (Cth), s 6(4), 11.

25 Department of Defence, *About the Defence Signals Directorate*, <www.dsd.gov.au/dsd/index.html> at 29 May 2003.

26 Department of Defence, *About the Defence Intelligence Organisation*, <www.defence.gov.au/dio> at 29 May 2003.

27 Department of Defence, *About the Defence Imagery and Geospatial Organisation*, <www.defence.gov.au/digo/> at 14 August 2003.

2.32 The Office of National Assessments (ONA), established by the *Office of National Assessments Act 1977* (Cth), falls within the portfolio responsibilities of the Prime Minister and provides information and advice directly to the Prime Minister. It produces reports and assessments on international political, strategic and economic matters. ONA assessments are based on information available from all sources, both inside and outside government, including intelligence, diplomatic reporting, media reports, academic commentary and other published material.[28]

2.33 Some law enforcement agencies also have a role in relation to national security. The Australian Federal Police (AFP), established by the *Australian Federal Police Act 1979* (Cth), is the primary Commonwealth law enforcement agency. The AFP falls within the portfolio responsibilities of the Minister for Justice and Customs. The AFP has responsibility for Commonwealth protective security and the prevention, detection and investigation of criminal offences against the Commonwealth, including national security-related offences. The Australian Protective Service (APS), a division of the AFP, is responsible for providing physical protective security in a range of situations including at Parliament House, sensitive defence establishments and foreign diplomatic missions, and for providing counter-terrorism first-response at airports.[29]

2.34 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, and falls within the portfolio responsibilities of the Minister for Justice and Customs. The ACC's functions include criminal intelligence collection and analysis; setting national criminal intelligence priorities; conducting intelligence-led investigations of criminal activity of national significance; and the exercise of coercive powers to assist in intelligence operations and investigations.[30]

2.35 Certain specialised divisions in various Australian Government departments also have a role to play in security and intelligence. The Protective Security Coordination Centre (PSCC) is part of the Criminal Justice and Security Group in the Attorney-General's Department. In the event of a terrorist incident, the PSCC would activate national crisis management arrangements and co-ordinate the national response while maintaining links between National Counter-Terrorism Committee (NCTC) members.[31] The PSCC also has several other special functions including the development, maintenance and co-ordination of Australia's national counter-terrorism capabilities; the provision of protective, physical, computer and personal security training to Commonwealth personnel; the provision of a security clearance advisory service to

28 Office of National Assessments, *About ONA*, <www.ona.gov.au> at 29 May 2003.

29 Australian Federal Police, *Australian Federal Police Home Page*, <www.afp.gov.au/> at 28 August 2003.

30 Australian Crime Commission, <www.crimecommission.gov.au/index> at 17 June 2003.

31 Attorney-General's Department, *National Counter-Terrorism Committee Communiqué*, 15 November 2002. The NCTC was established by intergovernmental agreement in October 2002. Committee members are drawn from relevant Commonwealth, State and Territory agencies. The role of the NCTC is to co-ordinate a nation-wide co-operative approach to counter-terrorism.

Commonwealth agencies; and the development and promotion of protective security policy and advice, including drafting and reviewing the PSM.

2.36 In late May 2003, the Australian Government announced that a new National Security Division was to be established within the Department of the Prime Minister and Cabinet. The Division is to focus on counter-terrorism, defence, intelligence, security, law enforcement and border protection. It will be responsible for co-ordinating whole-of-government approaches to national security issues and providing secretariat services to the Secretaries' Committee on National Security and the National Security Committee of Cabinet.[32]

2.37 In addition, in October 2003 the Attorney-General, the Hon Philip Ruddock MP, announced the establishment of the National Threat Assessment Centre (NTAC) to be located within ASIO. The NTAC will include staff seconded from the AFP, ASIS, the DIO, the Department of Foreign Affairs and Trade, the Department of Transport and Regional Services and the ONA. It will operate 24 hours a day to identify, and issue assessments of, threats to Australia, Australians and Australian interests both here and abroad. These assessments will form the basis for determining the national counter-terrorism alert level and will inform government decision-making about security measures.[33]

Oversight of activities

Inspector-General of Intelligence and Security

2.38 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office within the Prime Minister's portfolio established by the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act). The IGIS monitors the activities of the following intelligence and security organisations in Australia:

- Australian Secret Intelligence Service (ASIS);
- Australian Security Intelligence Organisation (ASIO);
- Defence Imagery and Geospatial Organisation (DIGO);
- Defence Intelligence Organisation (DIO);
- Defence Signals Directorate (DSD); and
- Office of National Assessments (ONA).

---

32 Department of the Prime Minister and Cabinet, *Organisational Restructure of the Department of the Prime Minister and Cabinet—Statement by Dr Peter Shergold, Secretary*, 23 May 2003.

33 The Hon Philip Ruddock MP (Attorney-General), *New Counter-Terrorism Intelligence Centre Launched*, Press Release, 17 October 2003.

2.39 The IGIS conducts inquiries, investigates complaints, makes recommendations to government and provides annual reports to the Australian Parliament.[34] Section 8 of the IGIS Act allows the Inspector-General to undertake inquiries in response to a complaint, at the request of the responsible 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.

2.40 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 to Parliament. 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.[35] Under s 20 of the Act, the Inspector-General may obtain documents with a national security classification for the purposes of an inquiry but must make arrangements with the head of the relevant agency for the protection of those documents while they remain in the Inspector-General's possession and for their return.

Parliamentary Joint Committee

2.41 The Parliamentary Joint Committee on ASIO, ASIS and the DSD is an amalgam of two previous separate Parliamentary committees overseeing those three agencies.[36] Its functions, as defined in s 29 of the *Intelligence Services Act*, are:

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

---

34 Inspector-General of Intelligence and Security, *About IGIS*, <www.igis.gov.au/fs_about.html> at 29 May 2003.

35 *Inspector-General of Intelligence and Security Act 1986* (Cth), s 18–19.

36 *Parliamentary Joint Committee on ASIO, ASIS and the DSD*, <www.aph.gov.au/house/committee/pjcaad/role.htm> at 29 May 2003.

- to review any matter in relation to ASIO, ASIS or the 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.

2.42 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.[37] The Joint Committee is specifically excluded from reviewing, among 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.

2.43 In response to a number of high profile espionage cases involving employees of Australia's intelligence agencies (Simon Lappas and Jean-Philippe Wispelaere), the IGIS conducted an inquiry into security arrangements in the relevant agencies. The Inspector-General's final report, *Inquiry Into Security Issues*, contained 50 recommendations and was submitted to the Prime Minister in March 2000. The report itself was not made public—even the Parliamentary Joint Committee on ASIO, ASIS and the DSD was not given formal access to the report. The intelligence agencies did provide details of relevant IGIS recommendations in their submissions to the Parliamentary Joint Committee during the preparation of its report, *Private Review of Agency Security Arrangements*,[38] tabled in Parliament on 13 October 2003, but the formal lack of access to the IGIS report was noted with disapproval by the Chair of the Committee, the Hon David Jull MP, who commented that:

> the lack of formal access to the IGIS inquiry report raises questions about the committee's ability to perform fully the functions assigned to it under the Intelligence Services Act and whether security concerns would inhibit the committee's ability to address other aspects of agency administration in future.[39]

Security Appeals Division of the AAT

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

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

---

37 Ibid.

38 Parliamentary Joint Committee on ASIO ASIS and DSD, *Private Review of Agency Security Arrangements* (2003).

39 Commonwealth, *Parliamentary Debates*, House of Representatives, 13 October 2003, 21151 (The Hon David Jull MP).

- applications under the *Archives Act 1983* (Cth) to review decisions refusing access to the whole or part of an ASIO document held by the National Archives of Australia.[40]

Overseas agencies

New Zealand

2.45 The New Zealand Security Intelligence Service (NZSIS) collects, analyses and assesses intelligence, including foreign intelligence, and provides advice on security issues to the New Zealand Government. It also provides advice to government agencies on security awareness, physical security and personnel security, including security clearances. The powers and functions of the NZSIS are set out in the *New Zealand Security Intelligence Service Act 1969* (NZ). The NZSIS is a civilian organisation. It has no police powers and no authority to enforce the law. The NZSIS traditionally falls within the Prime Minister's portfolio responsibilities.[41]

2.46 The Government Communications Security Bureau (GCSB) provides advice on all matters relating to foreign intelligence derived from the interception and exploitation of foreign communications and other signals. The GCSB also provides advice and services to the New Zealand Government on the security of its communications and information technology systems, and on the protection of premises and facilities from eavesdropping and other forms of technical attack. The *Government Communications Security Bureau Act 2003* (NZ) formally established the Bureau as a public service department and defines its objectives and functions. The GCSB, formerly within the Department of Defence, is now a separate agency and falls within the Prime Minister's portfolio responsibilities.[42]

2.47 The External Assessments Bureau, located in the Department of the Prime Minister and Cabinet, provides assessments on overseas events and developments. It draws on a wide range of information, including media reports, government communiqués, diplomatic reports, academic research and commentary, as well as intelligence gathered by the other security and intelligence agencies.[43]

2.48 The Directorate of Defence Intelligence and Security (DDIS) is the strategic arm of the New Zealand Defence Force's intelligence and security community. The DDIS is mainly concerned with foreign developments and the provision of intelligence and security advice to the Ministry of Defence and the Defence Forces.

---

40 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.

41 New Zealand Security Intelligence Service, *New Zealand Security Intelligence Service Home Page*, <www.nzsis.govt.nz/> at 28 August 2003. See also, more generally Department of the Prime Minister and Cabinet (NZ), *Security in the Government Sector*, <www.security.govt.nz/> at 28 August 2003.

42 Government Communications Security Bureau, *Government Communications Security Bureau Home Page*, <www.gcsb.govt.nz/> at 28 August 2003.

43 Department of the Prime Minister and Cabinet (NZ), *External Assessments Bureau Home Page*, <www.dpmc.govt.nz/eab/> at 28 August 2003.

2.49 The Inspector-General of Intelligence and Security, whose functions are set out in the *Inspector-General of Intelligence and Security Act 1996* (NZ), provides oversight and review of NZSIS, GCSB and any other agency declared by the Governor-General to be an intelligence and security agency for the purposes of the Act. In particular, the Inspector-General has power to inquire into whether the activities of these agencies comply with the law, and to investigate complaints by New Zealand citizens and employees of the agencies.

2.50 The Intelligence and Security Committee, established by the *Intelligence and Security Committee Act 1996* (NZ) and chaired by the Prime Minister, provides a level of parliamentary oversight and review of NZSIS, GCSB and any other agency declared by the Governor-General to be an intelligence and security agency for the purposes of the Act. The other members of the Committee are the Leader of the Opposition, two members of the House of Representatives nominated by the Prime Minister and one member of the House of Representatives nominated by the Leader of the Opposition, with the agreement of the Prime Minister. The Committee conducts its proceedings in private unless it unanimously decides otherwise.

United Kingdom

2.51 The British Security Service (also known as MI5) is the UK's domestic intelligence agency. It is responsible for security intelligence work in relation to threats to national security, including terrorism and espionage. Is role was expanded in 1996 to include support to law enforcement agencies in fighting serious crime although the Service itself has no police powers. In addition, MI5 provides protective security advice to a range of organisations both within and outside government. The *Security Service Acts* of 1989 and 1996 form the statutory basis for MI5, which falls within the responsibilities of the Home Secretary.[44]

2.52 The Secret Intelligence Service (SIS) (sometimes known as MI6) is responsible for the collection of intelligence overseas on behalf of the British Government. The SIS makes use of human and technical resources, as well as liaison with a wide range of foreign intelligence and security services. It was not officially recognised under statute until 1994, when it was brought under the *Intelligence Services Act 1994* (UK). The SIS falls within the responsibilities of the Foreign Secretary.

2.53 The Government Communications Headquarters (GCHQ) collects signals intelligence and information for government departments and law enforcement agencies. The Communications Electronics Security Group of GCHQ advises government departments and the armed forces on the security of their communications and information systems. GCHQ operates under the *Intelligence Services Act* and also falls within the responsibilities of the Foreign Secretary.

---

44 MI5, *Responsibilities of MI5*, <www.mi5.gov.uk/responsibilities/responsibilities.htm> at 29 May 2003. See also, more generally, Home Office (UK), *Terrorism*, <www.homeoffice.gov.uk/terrorism/> at 28 August 2003.

2.54 The Defence Intelligence Staff (DIS), part of the Ministry of Defence, analyses information from both overt and covert sources, and provides intelligence assessments, advice and strategic warnings to the Joint Intelligence Committee, the Ministry of Defence, Military Commands and deployed forces. Within the DIS, the Defence Geographic and Imagery Intelligence Agency and the Defence Intelligence and Security Centre are responsible for providing imagery, geographic products and intelligence training.

2.55 The Intelligence and Security Committee (ISC), established by the *Intelligence Services Act*, provides Parliamentary oversight of the Security Service, the SIS and GCHQ. The ISC examines the expenditure, administration and policy of the three agencies and has wide access to agency activities and to highly classified information. ISC members are appointed by, and report directly to, the Prime Minister, who tables their reports in the Parliament following the deletion of sensitive material.

2.56 The various agencies are also overseen by Commissioners, appointed under the *Regulation of Investigatory Powers Act 2000* (UK), who must hold, or have held, high judicial office. The Intelligence Services Commissioner reviews the issue and authorisation of warrants for operations by the agencies. The Interception Commissioner reviews the issue and authorisation of warrants to intercept mail and telecommunications by the intelligence and security agencies and law enforcement organisations. The Commissioners report annually to the Prime Minister on their work and the reports are then tabled in Parliament.[45]

2.57 The Commissioners assist the Investigatory Powers Tribunal established by the *Regulation of Investigatory Powers Act* to investigate public complaints against the security agencies and in relation to the interception of communications.[46] The Tribunal is made up of senior members of the legal profession or judiciary, who are appointed for five years. Since it was established in 2000, the Tribunal has received 71 cases, none of which has been determined in favour of the applicant.[47]

Canada

2.58 The Canadian Security Intelligence Service (CSIS) is a domestic civilian intelligence service established to collect and analyse information concerning threats to the security of Canada. The *Canadian Security and Intelligence Service Act 1984* (CSIS Act) defines 'threats to the security of Canada' to include espionage, sabotage, foreign influenced activities within Canada detrimental to national interests, and activities supporting violence for a political, religious or ideological objective.[48] CSIS is also responsible for conducting security assessments for all federal government departments and agencies (with the exception of the Royal Canadian Mounted Police) and immi-

45 The Cabinet Office (UK), *National Intelligence Machinery* (2001).
46 The Tribunal's powers to hold closed and secret hearings are discussed in Ch 9.
47 Intelligence and Security Committee (UK), *Intelligence Oversight* (2002).
48 *Canadian Security Intelligence Service Act 1985* RS 1985, c C-23 (Canada), s 2.

gration, citizenship and refugee applicants.[49] Canada does not have a security agency responsible for collecting intelligence overseas.[50]

2.59 The Royal Canadian Mounted Police (RCMP) is Canada's national police service and is responsible for enforcing federal laws. Until the creation of the CSIS as a separate agency in 1984, the RCMP was also responsible for the protection of national security. Under the *Security Offences Act 1984* (Canada), the RCMP continues to have primary investigative responsibility for offences related to terrorism and espionage. The RCMP also provides physical protection for the Governor General, the Prime Minister, and international visitors such as foreign heads of state. The RCMP's Criminal Intelligence Directorate collects and analyses intelligence to support criminal investigations, particularly those involving organised crime, high technology crime and illegal migration.[51]

2.60 The Director General Intelligence Division, in the Department of National Defence, provides defence intelligence on issues involving the use or potential use of the Canadian Forces abroad. It assesses foreign political and military information as well as scientific and technical information. The Communications Security Establishment (CSE), in the Department of National Defence, collects, analyses and reports on foreign signals intelligence. The CSE is also responsible for ensuring that the Canadian Government's telecommunications are secure from interception, disruption, manipulation or sabotage by others.

2.61 The Privy Council Office (PCO) provides advice and support to the Prime Minister, the Cabinet and Cabinet committees. Within the PCO, the Security and Intelligence Secretariat is responsible for policy advice to the Prime Minister on national security and foreign intelligence matters. The Intelligence Assessment Secretariat assesses conditions and trends in foreign countries, including the implications for Canadian policy makers.

2.62 The Inspector General of the CSIS, appointed under the CSIS Act, carries out internal, independent reviews of CSIS matters for the Solicitor General. The Inspector General monitors compliance with operational policies and reviews operational activities. The Security Intelligence Review Committee (SIRC) was established by the CSIS Act and is composed of three to five privy councillors.[52] It is responsible for ensuring that the CSIS uses its powers legally and appropriately. The Committee has access to

---

49 Canadian Security and Intelligence Service, <www.csis-scrs.gc.ca/eng/menu/faq_e.html> at 23 June 2003. See also, more generally, Privy Council Office, *The Canadian Security and Intelligence Community* (2001).

50 D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 505.

51 Royal Canadian Mounted Police, *Royal Canadian Mounted Police Home Page*, <www.rcmp-grc.gc.ca/> at 28 August 2003.

52 The Canadian Privy Council includes all Cabinet ministers and former Cabinet ministers, the Chief Justice and former chief justices, ex-Speakers of the House of Commons and a number of prominent citizens made members as a mark of honour. Membership of the Privy Council is for life unless a member is dismissed by the Governor General on the advice of the Prime Minister.

all documents under the control of CSIS, except those that are Cabinet-in-Confidence. The SIRC audits CSIS activity, and investigates complaints from the public. In addition, people denied a security clearance for federal employment, or denied federal contracts on security grounds, can complain to the SIRC. The Committee publishes its findings in an annual report to Parliament. There is no direct parliamentary oversight of CSIS activity.[53]

2.63 The Commission for Public Complaints Against the RCMP was established in 1988 to receive complaints about the conduct of RCMP members in the performance of their duties. The Commission reviews complaints and makes recommendations to the Commissioner of the RCMP. The chair of the Commission has the authority to conduct an independent investigation or to hold a public hearing.

2.64 The Communications Security Establishment Commissioner reviews the activities of the CSE to determine whether they are in compliance with the law. The Commissioner is independent of the CSE and has access to all CSE personnel and records (except those that are Cabinet-in-Confidence). The CSE Commissioner must inform the Minister of National Defence and the Attorney General of Canada of any activity that may not comply with the law. The Commissioner can also respond to complaints from the public about the CSE. The Commissioner provides an annual report to the Minister of National Defence, which is tabled in Parliament.

United States

2.65 There are a relatively large number of agencies involved in security and intelligence work in the United States, including the Department of Homeland Security established in late 2001.

2.66 The Central Intelligence Agency (CIA) is perhaps the best known of these agencies and was established by the *National Security Act 1947* (US). The CIA collects intelligence overseas, provides advice on national security issues and conducts counter-intelligence activities, 'special activities', and other functions related to foreign intelligence and national security. Unlike the other intelligence agencies described above, the CIA has a mandate to engage in covert operations in other countries.[54] The Director of Central Intelligence leads the CIA and is also the head of the US intelligence community as a whole. The CIA reports through the Director to the President.[55]

2.67 The Federal Bureau of Investigation (FBI) is the investigative arm of the US Department of Justice. It is a law enforcement agency with police powers and is responsible for enforcing federal criminal law. The National Security Division of the FBI has responsibility for counter-intelligence and counter-terrorism within the United

---

53 D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 511.

54 Ibid, 520.

55 Central Intelligence Agency, *Central Intelligence Agency Home Page*, <www.cia.gov/> at 28 August 2003. See also, more generally, US Government, *United States Intelligence Community*, <www.intelligence.gov> at 28 August 2003.

States, as well as collecting information about activity which threatens national security, espionage investigations and the arrest of international terrorists charged with violating US laws overseas. The FBI also conducts security checks in relation to nominees for sensitive government positions.[56]

2.68 The National Security Agency (NSA) is responsible for providing foreign signals intelligence, designing cipher systems to protect the integrity of US information systems and searching for weaknesses in adversaries' systems and codes. NSA also provides advice on the protection of classified and sensitive information that is stored or sent through the US. The NSA is administered by the Department of Defense.

2.69 The Defense Intelligence Agency (DIA) is responsible for providing co-ordinated advice to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff on military intelligence matters. The DIA plays a key role in providing intelligence on foreign weapon systems to assist weapon systems planners and defence acquisition programs.

2.70 The National Reconnaissance Office (NRO) was established in 1960 to develop satellite reconnaissance systems. The NRO is responsible for the engineering, development, acquisition, and operation of space reconnaissance systems and related intelligence activities. The NRO is an agency of the Department of Defense.

2.71 The National Imagery and Mapping Agency is also an agency of the Department of Defense. It provides geospatial intelligence derived from the analysis of imagery and geospatial information to describe, assess, and visually depict physical features and activities.

2.72 In late 2001, the US Government established the Department of Homeland Security, drawing together 22 existing domestic agencies with the intention of better co-ordinating efforts to prevent further terrorist attacks. The Department has a wide range of responsibilities including analysing threats and intelligence, guarding borders and airports, protecting critical infrastructure, and co-ordinating the response to future emergencies.[57]

2.73 Two Congressional Committees—the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence—oversee the US intelligence agencies and their activities. These committees assess and report to Congress on whether the agencies are providing informed and timely intelligence and whether their activities are consistent with the US Constitution and other laws. In February 2002, the committees agreed to conduct a joint inquiry into the effectiveness of the US intelli-

---

56 Federal Bureau of Investigation, *Federal Bureau of Investigation Home Page*, <www.fbi.gov/homepage.htm> at 28 August 2003.

57 US Government, *United States Intelligence Community*, <www.intelligence.gov> at 28 August 2003.

gence community in connection with the terrorist attacks on 11 September 2001. The Joint Inquiry's final report was published in December 2002.[58]

58 US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (2002).

3. Open Government

Contents

Accountability of the Executive

3.1 It is a central tenet of representative democracies that the government is open to account for its actions, policies and administrative decisions. A key part of this accountability is public access to the information on which action and policies are based:

> Australia is a representative democracy. The Constitution gives the people ultimate control over the government, exercised through the election of the members of Parliament. The effective operation of representative democracy depends on the people being able to scrutinise, discuss and contribute to government decision making. To do this, they need information.[1]

3.2 A more open working environment helps to provide checks and balances that are necessary to discourage corruption and misconduct, and to sustain a healthy liberal democracy. The first annual report under the *Freedom of Information Act 1982* (Cth) stated the following three goals to be achieved by more open government:

- to improve the quality of agency decision making;
- to enable citizens to be kept informed of the functioning of the decision making process as it affects them and to know the criteria that will be applied in making these decisions; and

1 Australian Law Reform Commission and Administrative Review Council (Joint Inquiry), *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77/ARC 40 (1995), 12.

- to develop the quality of political democracy by giving all Australians the opportunity to participate fully in the political process.[2]

3.3 Balanced against this is the legitimate public interest in maintaining the confidentiality and secrecy of some official government information. Achieving an appropriate balance may be particularly difficult in respect of classified and security sensitive information:

> 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.[3]

3.4 This issue has arisen recently for consideration in the case of *Bennett v President, Human Rights and Equal Opportunity Commission*.[4] On 10 December 2003, Finn J of the Federal Court of Australia declared invalid reg 7(13) of the *Public Service Regulations 1998*—which imposed a very broad obligation of secrecy on Commonwealth officers in relation to official information—on the basis that it infringed the implied constitutional freedom of political communication. Finn J held that the regulation failed the test set out by the High Court in *Lange v Australian Broadcasting Corporation*[5] in that:

- it was a law that burdened the freedom of public servants to disseminate information and to make communications about government and political matters; and

- due to the breadth of the provision, it was not reasonably and appropriately adapted to serve a legitimate end, the fulfilment of which was compatible with the maintenance of the system of government prescribed by the *Constitution*.

3.5 Finn J acknowledged that there was a legitimate public interest in protecting some official information. However, he was of the view that the regulation under consideration was cast too broadly and did not adequately balance the need for secrecy with the competing public interest in allowing free discussion of government and political issues.[6]

3.6 Another area in which the need to protect official information and the need for access to that information may come into conflict is in court and tribunal proceedings. Claims of public interest immunity frequently arise in that context—including, on

---

2 Ibid, 11–12.

3 H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995), 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.' Relevant extracts from the US Constitution are set out in Appendix 3.

4 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433.

5 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

6 This decision and its implications are discussed further in Ch 4 and 5.

occasion, in relation to classified and security sensitive information. This is a central focus of this inquiry and is discussed in detail in Chapters 7 to 10.

3.7 A number of existing legislative regimes also regulate access to government information. At the federal level these include the *Privacy Act 1988* (Cth) and the *Freedom of Information Act 1982* (Cth). While a general review of the operation of these regimes is outside the scope of this inquiry, both Acts contain relevant exemptions in relation to information that would prejudice Australia's security, defence or international relations. These exemptions are likely to apply in relation to a great deal of classified and security sensitive information, and are discussed in some detail below.

3.8 The regime established by the *Archives Act 1983* (Cth) for the storage of, and public access to, government records is also relevant and is discussed in Chapter 4.[7]

3.9 One further element in an effective system of open government is providing protection for legitimate 'whistleblowers'—people who disclose official information in the public interest. The protection of whistleblowers may involve 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 reprisals, where it will assist in the elimination of incompetent or improper conduct by government officials. Whistleblowers' protection is considered further in this Chapter.

Privacy

3.10 The *Privacy Act* aims to protect personal information about individuals and give them some control over how that information is collected, stored, used and disclosed. It also gives individuals rights to access and correct their own personal information.[8]

3.11 The *Privacy Act* contains safeguards set out in a number of Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), which have the force of law.[9] The IPPs cover '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 Australian Government and ACT public sector entities. The NPPs cover personal information held by certain private sector organisations.[10]

---

7 The ALRC has considered a number of these issues in the past: Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979); Australian Law Reform Commission, *Privacy*, ALRC 22 (1983); Australian Law Reform Commission and Administrative Review Council (Joint Inquiry), *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77/ARC 40 (1995); Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998).

8 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).

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

10 The *Privacy Amendment (Private Sector) Act 2000* came into operation on 21 December 2001 and extended the coverage of the *Privacy Act* to much of the private sector. The private sector provisions of the *Privacy Act* apply to 'organisations', which include partnerships, unincorporated associations and bodies

3.12 The Federal Privacy Commissioner has a number of statutory functions in relation to the handling of complaints, investigating breaches of the Act, and enforcement. Under Part V of the Act, the Commissioner has the power to investigate complaints,[11] obtain information and documents[12] and examine witnesses.[13] The Commissioner's determinations may be enforced by proceedings in the Federal Court of Australia or the Federal Magistrates Court.[14]

3.13 The *Privacy Act* regime is not directly concerned with issues of national security. However, NPP 6.1 provides a relevant exemption to the NPPs 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.

3.14 In addition, the *Privacy Act* limits the power of the Federal Privacy Commissioner to require the production of certain information. Under s 70, the Attorney-General may issue a certificate to the effect that the giving of specific information to the Commissioner would be contrary to the public interest on a number of grounds, including that it would prejudice Australia's security, defence or international relations.

---

corporate. An individual who is self-employed or a sole trader is considered an organisation for the purposes of the *Privacy Act*. Organisations are generally responsible for the actions of their employees, contractors and subcontractors, all of which are covered by the *Privacy Act:* s 6C, 8.

11 *Privacy Act 1988* (Cth), s 40.

12 Ibid, s 44.

13 Ibid, s 45.

14 Ibid, s 55A.

The Federal Privacy Commissioner has informed the ALRC that this provision has not been invoked to date.[15]

3.15 The ALRC has not received any evidence or submissions suggesting that these exemptions require reform. Consequently, no proposals are made in this Discussion Paper in relation to the *Privacy Act*.

Freedom of information

3.16 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 as a legitimate aspect of government decision making.

3.17 Section 7 of the FOI Act provides a complete exemption from the provisions of the *Freedom of Information Act* for certain agencies including the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), the Office of National Assessments (ONA) and the Inspector-General of Intelligence and Security (IGIS). Other organisations are exempt in relation to certain documents. For example, the Department of Defence is exempt in relation to documents in respect of the activities of the Defence Intelligence Organisation (DIO) and the Defence Signals Directorate (DSD).

3.18 Other Commonwealth agencies that handle a significant amount of material relating 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, are open to freedom of information applications. However, s 7(2A) provides an exemption for all agencies in relation to documents that originate with, or have been received from, ASIS, ASIO, ONA, DIO, DSD or the IGIS.

3.19 In addition, 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; for example, s 33(1) provides that:

> 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.

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

3.20 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.

3.21 Section 33(2) provides that, where a Minister is satisfied that a document is an exempt document for a reason referred to in s 33(1), he or she may sign a certificate to that effect. Such a certificate, so long as it remains in force, establishes conclusively that the document is an exempt document. A decision to exempt in this fashion can be reviewed by the Administrative Appeals Tribunal (AAT).[16]

3.22 In *Re Anderson and the Australian Federal Police*, the AAT examined claims for exemption by the AFP which were not based on national security but rather on, among other things, protection of witnesses, sources and investigation techniques.[17] 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.[18]

3.23 It has been argued that the many exemptions to access rights under FOI laws result in very restricted access to information that might have national security implications. In contrast, the *Freedom of Information Act* in the United States contains no blanket exemption of security intelligence agencies and its exemption for security sensitive information is subject to judicial review.[19] However, in 2001 US Attorney General John Ashcroft 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.[20]

---

16 *Freedom of Information Act 1982* (Cth), s 55(1), 58(1).
17 *Re Anderson and the Australian Federal Police* (1986) 11 ALD 355.
18 Ibid, [120].
19 H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995), 124.
20 J Ashcroft, *Memorandum for Heads of all Federal Departments and Agencies re The Freedom of Information Act*, 12 October 2001.

3.24 In 1995, the ALRC and the Administrative Review Council (ARC) published the final report of their joint inquiry into the *Freedom of Information Act*.[21] The inquiry reviewed the form and operation of the entire Act, including the exemptions discussed above, and reached a number of conclusions relevant to the present inquiry.

3.25 The ALRC and ARC concluded that it was appropriate to exempt ASIS, ASIO, ONA and the IGIS from the operation of the FOI Act. This was justified on the basis that the intelligence agencies' internal processes and methods were scrutinised by the IGIS and by the relevant Parliamentary committee. In view of the fact that the vast majority of their documents would be exempt even if they were subject to the Act, these accountability mechanisms were considered to be adequate.[22]

3.26 The Report stated, however, that s 33 of the FOI Act provided sufficient protection for documents relating to the work of DIO and DSD and recommended that the Department of Defence should be required to demonstrate to the Attorney-General that such documents warranted specific exclusion from the Act.[23]

3.27 The Report noted that s 33 was not subject to a public interest test but considered this appropriate, except in respect of information communicated in confidence by an international organisation. The Report concluded that, in order for the Australian Government to function effectively in the international political arena, it was essential that it could give an absolute guarantee that information received in confidence from other governments would remain confidential. The Report did not consider that information received from international organisations warranted the absolute protection afforded to information from foreign governments, and recommended that s 33(1)(b) of the Act be divided and that a public interest test be introduced into the exemption insofar as it relates to international organisations.[24]

3.28 The Report also considered that conclusive ministerial certificates were justified in respect of s 33 national security and defence issues.[25]

3.29 The ALRC has not received any evidence or submissions in response to the questions asked in BP 8[26] about whether these exemptions require further review. No proposals are made in this Discussion Paper in this regard, but the ALRC remains interested in receiving feedback on these issues.

---

21 Australian Law Reform Commission and Administrative Review Council (Joint Inquiry), *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77/ARC 40 (1995).
22 Ibid, 152.
23 Ibid, 153.
24 Ibid, 106.
25 Ibid, 99.
26 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003).

Protection of whistleblowers

3.30 One further element in an effective system of open government is providing protection for 'whistleblowers' from some of the consequences that might normally follow such disclosures, such as prosecution for breach of a secrecy provision, the imposition of administrative or disciplinary sanctions, or other reprisals. In September 2002, the Senate Finance and Public Administration Legislation Committee (the Senate Committee), in considering the Public Interest Disclosure Bill 2001 [2002],[27] noted that:

> Whistleblowing or public interest disclosure schemes rest on the premise that individuals who make disclosures serve the public interest by assisting in the elimination of fraud, impropriety and waste. An effective whistleblowing scheme is a necessary part of maintaining a good public administration framework ...
>
> The objective [is] 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.[28]

Public interest disclosure legislation in Australia

3.31 Most Australian States and Territories have some form of public interest disclosure legislation to regulate and protect whistleblowers.[29] These laws limit the liability of people who make public interest disclosures and the legal action that can be taken against them on the basis of having made such disclosures.[30] These laws also provide for prosecution in the event of unlawful reprisals against whistleblowers,[31] and for whistleblowers to seek damages if they suffer reprisals.[32]

---

27 The Public Interest Disclosure Bill 2001 [2002] was a Private Senator's Bill introduced into Parliament by Senator Andrew Murray on 27 June 2001. The Senate Finance and Public Administration Legislation Committee considered the Bill in detail and, while supporting the general intent of the Bill, was of the view that some of the provisions required reconsideration and redrafting. Following consideration by the Senate Committee, Senator Murray made a number of amendments and introduced the Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 into the Senate on 11 December 2002.

28 Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, 3.

29 These include the *Whistleblowers Protection Act 1993* (SA), the *Protected Disclosures Act 1994* (NSW), 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 *Public Interest Disclosure Act 2003* (WA). There is no legislation in the Northern Territory providing protection for whistleblowers. However, the Northern Territory Law Reform Committee has 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.

30 See, for example, *Protected Disclosures Act 1994* (NSW), s 21, which 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'.

31 See, for example, Ibid, s 20 and *Whistleblowers Protection Act 2001* (Vic), s 18.

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

3.32 At the federal level, s 16 of the *Public Service Act*, 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[33] to:
>
> (a) the Commissioner or a person authorised for the purposes of this section by the Commissioner; or
>
> (b) the Merit Protection Commissioner 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.[34]

3.33 Division 2.2 of the *Public Service Regulations 1999*, also deals with public interest disclosures and provides more detail in relation to procedures for dealing with whistleblowers' reports.

3.34 However, the Senate Committee noted in its report on the Public Interest Disclosure Bill 2001 that:

> While the *Public Service Act 1999* provides some coverage for Commonwealth public sector whistleblowers, the Act only applies to about half of the Commonwealth public sector.[35]

3.35 For example, ASIO staff are employed under the *Australian Security Intelligence Organisation Act 1979* (Cth) on the basis of written contracts with the Director-General of Security. Section 86 of the Act makes it clear that ASIO officers and employees are not subject to the *Public Service Act*. However, the Act does not include any whistleblower protection.

3.36 ASIS staff are employed under the *Intelligence Services Act 2001* (Cth) on the basis of written contracts with the Director-General of ASIS. Section 35 of that Act 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.

---

33 The APS Code of Conduct is set out in the *Public Service Act 1999* (Cth), s 13. The Code of Conduct is discussed in Ch 4 and is set out in Appendix 3.

34 Section 7 defines 'Commissioner' as the Public Service Commissioner appointed under the *Public Service Act*. The 'Merit Protection Commissioner' is also appointed under the Act.

35 Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, 1.

3.37 While the Director-General of ASIS may adopt the principles of the *Public Service Act*, ASIS staff are not directly covered by the whistleblower protection provided by s 16 of that Act.

3.38 Australian Federal Police (AFP) officers are employed under the *Australian Federal Police Act 1979* (Cth). Section 66 of that Act provides limited protection for members of the AFP from civil or criminal proceedings arising from a work report made in good faith to someone who had a duty, or whose function it was, to receive such reports. The AFP stated in its submission that:

> One of the integrity and accountability measures utilised within the AFP is the maintenance and promotion of a Confidant Network, to encourage the notification and addressing of any matters of ethical or other concern within the organisation. This allows for the maintenance of protection to classified and security sensitive material within the AFP and provides a degree of protection to the person raising the concern.[36]

3.39 Civilian staff of the Department of Defence (including the Defence Signals Directorate (DSD), the Defence Intelligence Organisation (DIO) and the Defence Imagery and Geospatial Organisation (DIGO)), the staff of the Inspector-General of Intelligence and Security and the staff of the Office of National Assessments (ONA) are employed under the *Public Service Act* and enjoy the protection provided by s 16 of that Act.

3.40 The Inspector-General of Intelligence and Security has the power to conduct inquiries in response to complaints about the activities of ASIO, ASIS, DSD and, to a more limited extent, into the activities of DIO and ONA. These powers include, in relation to ASIO, ASIS and DSD, the power to inquire into compliance by those agencies with the law and with directions and guidelines issued by the Minister, and into the propriety of their activities.[37] While this provides one avenue for staff of these organisations and others to expose fraud, impropriety and waste, the *Inspector-General of Intelligence and Security Act* does not provide whistleblower protection for individuals making such disclosures, although s 33 provides some protection from civil actions.

3.41 In examining the Public Interest Disclosure Bill 2001 [2002], the Senate Committee expressed the view that there were sound reasons for allowing public interest disclosures to be made to external, independent bodies, and recommended that these should include the Commonwealth Ombudsman.[38] The Gibbs Committee Review of Commonwealth Criminal Law, in its final report recommended that, in relation to ASIO, ASIS and DSD, the Inspector-General of Intelligence and Security should also be included.[39]

---

36 Australian Federal Police, *Submission CSSI 13*, 18 September 2003.

37 *Inspector-General of Intelligence and Security Act 1986* (Cth), s 8.

38 Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, 51.

39 Attorney-General's Department, *Review of Commonwealth Criminal Law: Final Report* (1991), 338.

Public interest disclosure legislation overseas

United States

3.42 In the US, 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.[40]

3.43 In 2002, 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. Agent Rowley testified before Congress that supervisors in FBI headquarters impeded attempts by agents in Minneapolis to obtain a warrant to examine Moussaoui's laptop computer, which was found to contain information suggesting his complicity in the attacks. As FBI agents are not covered by whistleblower legislation, members of the Senate requested the US Attorney General to promise that Agent Rowley would not face reprisals for her testimony.[41]

3.44 Employees of the US Department of Homeland Security are covered by whistleblower protections.[42] Early versions of the law establishing the Department did not include such protections. However, Senator Chuck Grassley (Republican–Iowa) insisted that the whistleblower protections be added to the final Bill.[43] Senator Grassley is a co-author of the *Whistleblower Protection Act 1989* (USA). In arguing for whistleblower protection for staff at the Department of Homeland Security, he 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.[44]

New Zealand

3.45 New Zealand's *Protected Disclosures Act 2000* covers public interest disclosures within both public and private sector organisations, and provides protection for

---

40 T Wang, *The New Homeland Security Agency and Whistleblowers* (2002) The Century Foundation, 4.
41 Ibid, 2.
42 *Homeland Security Act 2002* (USA), s 883.
43 J Peckenpaugh, *Homeland Security Employees Will Retain Whistleblower Rights*, <http://foi.missouri.edu/whistleblowing/homelandsecurity1.html> at 20 November 2002.
44 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> at 26 June 2002.

those who bring such information forward in accordance with the procedures set out in the Act. The Act does extend whistleblower protection for disclosures to the staff of the intelligence and security agencies, but special procedures are provided in relation to these agencies.[45]

3.46 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.

3.47 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. These provisions mean that, in order to receive the protection of the *Protected Disclosures Act*, disclosures relating to an intelligence and security agency must go only to the Inspector-General of Intelligence and Security. Disclosures arising from within the Department of the Prime Minister and Cabinet, the Ministry of Foreign Affairs and Trade, the Ministry of Defence, or the New Zealand Defence Force, where they relate to the international relations of the Government or to intelligence and security matters, must be made only to an Ombudsman.

United Kingdom

3.48 The UK *Public Interest Disclosure Act 1998* inserted public interest disclosure provisions into the *Employment Rights Act 1996* (UK), which applies to workers in public and private sector organisations. It provides protection for those who bring such information forward in accordance with the procedures set out in the Act. However, the Act expressly excludes staff of the British Security Service, the Secret Intelligence

45 *Protected Disclosures Act 2000* (NZ), s 12–14.

Service, the Government Communications Headquarters, the police and the defence forces.

Consultations and submissions

3.49 The Australian Federal Police submitted that:

> The provision of an independent authority with appropriate security clearance, to which information may be disclosed by persons believing on reasonable grounds that this is in the public interest and unable to be addressed via internal reporting mechanisms, would promote integrity and accountability without releasing such information into the public domain.[46]

3.50 The Australian Crime Commission (ACC), however, warned that:

> Extending whistleblower protection to high risk Commonwealth agencies like the ACC presents difficulties for such agencies whose opponents have the capability to use disaffected agency staff to make public sensitive information. The ACC has a complaint handling procedure settled with and involving the Commonwealth Ombudsman which is regarded as an appropriate channel for responding to complaints from within the ACC.[47]

3.51 The Law Council of Australia submitted that existing Commonwealth provisions relating to whistleblowing were inadequate, acknowledging that:

> it may be necessary to create specific procedures in relation to public interest disclosures where security sensitive or classified information is involved. This may even require the advent of specialised tribunals or designated agencies to hear and investigate reports in cases involving such information.[48]

Commission's views

3.52 In ALRC 82,[49] the ALRC recommended legislation to protect and encourage whistleblowers, and that such legislation should cover all Commonwealth agencies. This position is consistent with the recommendations of a number of committees and inquiries into this issue in Australia in the last 15 years, including the Gibbs Committee Review of Commonwealth Criminal Law.[50]

---

46 Australian Federal Police, *Submission CSSI 13*, 18 September 2003.

47 Australian Crime Commission, *Submission CSSI 15*, 13 October 2003.

48 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

49 Australian Law Reform Commission, *Integrity: But Not by Trust Alone*, ALRC 82 (1996), Rec 117.

50 Attorney-General's Department, *Review of Commonwealth Criminal Law: Final Report* (1991). In 1993, the House of Representatives Standing Committee on Banking, Finance and Public Administration reported on its inquiry into fraud in the Commonwealth. It also found a need for the Commonwealth to implement a scheme to facilitate the disclosure of information in the public interest. In August 1994, the Senate Select Committee on Public Interest Whistleblowing tabled its report recommending that 'the practice of whistleblowing should be the subject of Commonwealth legislation to facilitate the making of disclosures in the public interest and to ensure protection for those who choose so to do.'

3.53 The ALRC agrees with the submission by the AFP that public interest disclosure mechanisms are essential to promote integrity and accountability within organisations, including those organisations dealing with classified and security sensitive information.

3.54 Where public interest disclosures involve classified or security sensitive information, the procedures for disclosure need to take into account the public interest in providing adequate protection for such information. This does not mean, however, that there should be no avenues for whistleblowing. Where no formal avenues are provided for individuals who believe that information they hold must be disclosed in the public interest, those individuals may well feel forced to find other ways to make the information known outside the organisation, such as through the media. It is much better to provide a more secure, structured, fair outlet for whistleblowing through the Inspector-General of Intelligence and Security. This would meet both public interests in the disclosure of improper actions by government officers and in the protection of legitimate classified and security sensitive information.

3.55 The ALRC notes the ACC's concern in relation to agencies dealing with sensitive information, but considers that it would be possible to develop procedures for dealing with public interest disclosures from such agencies. The NZ *Protected Disclosures Act* provides one possible model.

Proposal 3–1 The Australian Government should legislate to introduce a comprehensive public interest disclosures scheme. The scheme should cover all Australian Government agencies, including the security and intelligence agencies. The scheme should provide special procedures for dealing with disclosures from and about the intelligence and security agencies and concerning classified and security sensitive information. These procedures should be designed to ensure that classified and security sensitive information is adequately protected and at the same time:

(a) encourage public interest disclosures;

(b) ensure that such disclosures are independently investigated; and

(c) ensure that those making such disclosures are protected from reprisals.

PART B

Handling Classified and Security Sensitive Information

4. Commonwealth Protective Security Manual

Contents

4.1 A 1999 report by the Australian National Audit Office (ANAO) concluded that:

> In the opinion of the ANAO, all organisations covered by the audit were not adequately *protecting the confidentiality of sensitive information* in accordance with the Commonwealth's security classification system, related Government policy and standards, and recognised best practice. While the extent of the breakdowns in information security varied among the organisations, the more common and serious breakdowns related to risk assessments and planning, allocation of responsibility, IT&T networks, security clearances, staff training and awareness, and monitoring and review activities. As a result, there was a high risk of unauthorised access to sensitive information within most of the organisations examined. This was particularly so in relation to staff and other people dealing with the organisations, such as contractors and clients. This level of risk is considered significant given the nature of the information and the likely consequences, if it were misused.[1]

4.2 The primary issue for this Inquiry is the need to examine measures to protect classified and security sensitive information in the course of court and tribunal proceedings. Chapters 7 to 10 of this Discussion Paper will consider this issue, including the mechanisms available to prevent or limit inappropriate disclosure of such information in the course of proceedings. However, the Terms of Reference also specifically

1 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), 13. See also [4.21] below.

ask the ALRC to examine whether the protective security standards set out in the *Commonwealth Protective Security Manual* (PSM)[2] are enforceable. This element of the reference is concerned with the handling and protection of classified and security sensitive information in the course of everyday government business,[3] rather than in the course of court or tribunal proceedings.

4.3 As acknowledged in the PSM, the protective security standards it sets out are not enforceable *per se*.[4] The PSM is a policy document without legally binding force. This chapter examines the protective security measures set out in the PSM and considers the extent to which those measures, and the way they are currently implemented, are effective in providing adequate protection for classified and security sensitive information. This chapter also examines whether those protective security measures are, or should be made, mandatory for, and enforced against, Australian Public Service (APS) officers, as well as contractors and their employees.

4.4 Chapter 5 provides a detailed consideration of the legislative provisions and other legal mechanisms available to prevent or punish unauthorised disclosures of official information and the extent to which those mechanisms may assist in protecting classified and security sensitive information.

4.5 Court proceedings to prevent unauthorised disclosure of sensitive information and to punish individuals for making such disclosures may go some way towards encouraging compliance with protective security standards. The PSM advocates a more comprehensive and preventive approach to the issue, however, by seeking to ensure that such information is dealt with in an appropriate security environment. This involves establishing a range of routine practices and procedures for handling sensitive information in the administrative context that operate to prevent such disclosures from occurring in the first place. In protecting classified and security sensitive information, prevention is obviously a much more effective mechanism than punishment.

What is the Protective Security Manual?

4.6 The Attorney-General is responsible for the Australian Government's protective security policy. The PSM is produced and periodically revised by the Protective Security Coordination Centre (PSCC) in the Attorney-General's Department.

> [The PSM] 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.[5]

---

2 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000).

3 Including investigations, which are specifically mentioned in the Terms of Reference: see p 5.

4 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), A 18, [5.1]; C 19, [4.17].

5 Attorney-General's Department, *Protective Security Coordination Centre Home Page*, <www.ag.gov.au/www/protectivesecurityhome.nsf> at 29 August 2003.

4.7 The PSM sets out guidelines and minimum standards in relation to protective security for all Australian Government agencies and officers, and for contractors and their employees who perform services for or on behalf of the Australian Government. It is of particular relevance to agencies concerned with national security matters and law enforcement.

4.8 The PSM is divided into eight sections:

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.

4.9 The PSM contains a mix of broad statements of policy, guidelines and, in some cases, quite detailed procedural standards and requirements. Part C of the PSM, which deals with information security, is of particular relevance. It describes the Government's information classification system in relation to national security and non-national security information.[6]

> The security classification system has been devised primarily to ensure that official information held by, or shared between, Commonwealth agencies receives adequate protection based on the degree of harm that could be caused to the Commonwealth in the event of unauthorised disclosure of the information.[7]

4.10 Part C sets out the following information security principles:

- The availability of information should be limited to those who need to use or access the information to do their work. This principle is commonly referred to as the need-to-know principle.[8]

- 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.[9]

- Once information has been identified as requiring security classification, a protective marking must be assigned to the information.[10]

---

6 The difference between national security and non-national security information and the various protective markings that may be applied are discussed in detail in Ch 2.
7 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), A 4, [4.1].
8 Ibid, C 9, [2.4].
9 Ibid, C 10, [2.7].
10 Ibid, C 30, [6.26].

- Once information has been security classified, agencies must observe the minimum procedural requirements for its use, storage, transmission and disposal.[11]

4.11 Minimum procedural requirements are also set out in Part C; for example:

- 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.[12]

- Agencies should provide a system of document registration that identifies all security classified information held by the agency, including details of creation, location and disposal. Agencies must have a security classified document register in relation to information classified Top Secret.[13]

- Files must carry the protective marking of the highest level of security classified information they contain. It is recommended that files containing classified information are standard colours: post office red for Top Secret, salmon pink for Secret, green for Confidential, and blue or buff for Restricted.[14]

4.12 Other minimum standards address matters of copying, storage and disposal of classified information, removal from agency premises, manual and electronic transfer or transmission, and IT security issues.

4.13 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 in certain limited circumstances. The waiver may be sought only for a defined purpose and for a nominated period of time.[15] Alternatively, an Agency Head may choose to implement standards in excess of those prescribed in the PSM.[16]

Public access to the PSM

4.14 The PSCC website indicates that, although the PSM itself is not a classified document, access to it is restricted to government departments, agencies and contractors working for the government.[17] The ALRC understands that this is because some parts of the PSM are thought to be unsuitable for unrestricted publication.

---

11 Ibid, C 10, [2.8].
12 Ibid, C 26, [6.9].
13 Ibid, C 48, [7.13].
14 Ibid, C 49, [7.24].
15 Ibid, A 6, [1.9].
16 Ibid, A 16, [4.6].
17 Attorney-General's Department, *Protective Security Coordination Centre Home Page*, <www.ag.gov.au/www/protectivesecurityhome.nsf> at 29 August 2003.

4.15 By way of contrast, the Defence Signals Directorate (DSD) publishes the *Australian Communications Electronic Security Instruction (ACSI) 33* on its website.[18] This document provides guidance to Australian Government agencies on the protection of their electronic information systems and contains information of much the same order as the PSM. It includes separate handbooks on standards, risk management, network security, cryptographic systems, and so on. The Supplement to Handbook 14 on Physical Security is currently classified Restricted and is not freely available. In several places, ACSI 33 asks users to refer to the DSD for further information, presumably where it would be inappropriate to place more detailed information in the public arena. For example:

> National security classified information at **CONFIDENTIAL**, **SECRET** or **TOP SECRET** markings must be encrypted using Government Furnished Encryption (GFE) systems. The algorithms described above are ***not*** suitable. Details on the use of GFE for protection of national security classified information are available from DSD.[19]

4.16 ACSI 33, which is to be renamed the Government IT Security Manual, is currently being revised and is scheduled for release at the *Security in Government* conference in March 2004. Three versions of the new draft ACSI 33 have been circulated for comment: a public version, as well as security-in-confidence and confidential versions. The public version covers IT systems in the public domain, unclassified, In-Confidence, Restricted and Protected classifications. The security-in-confidence version covers all of these as well as Highly Protected, and the confidential version covers all of these as well as Confidential and higher classifications.

4.17 The New Zealand Government's equivalent security manual, *Security in the Government Sector*—which includes content based on the PSM—is publicly available.[20] The Canadian Government Security Policy,[21] and related documents such as the *Physical Security Standard*[22] and the *Security Organisation and Administration Standard*,[23] are also publicly available. In the United States, Executive Order 12958 *Classified National Security Information*,[24] discussed further below,[25] is on the public record. The United Kingdom's *Manual of Protective Security* and *Information Security Standards*, however, are not generally available—although the ALRC has been

---

18 Defence Signals Directorate, *Australian Communications—Electronic Security Instruction (ACSI) 33* (2000).

19 Ibid.

20 Department of the Prime Minister and Cabinet (NZ), *Security in the Government Sector* (2002).

21 Treasury Board of Canada Secretariat, *Government Security Policy*, 1 February 2002.

22 Treasury Board of Canada Secretariat, *Physical Security Standard 2–02*, 15 November 1994.

23 Treasury Board of Canada Secretariat, *Security Organization and Administration Standard 2–01*, 1 June 1995.

24 *Executive Order 12958—Classified National Security Information*, 17 April 1995. EO 12958 has been amended on two occasions, most recently in March 2003. The references to EO 12958 in this Report are to the Order as amended.

25 See [4.27]–[4.28], [4.47]–[4.51] and [4.111] below.

informed that the UK manual contains considerably more detail than its Australian counterpart about the selection and implementation of security controls.[26]

4.18 The various mechanisms adopted by the DSD in relation to the current and draft future versions of ACSI 33 ensure that introductory and general policy information in relation to the protection of government IT systems is publicly available while genuinely sensitive information is protected. Adopting a similar approach in relation to the PSM would be consistent with the Australian Government's policy as stated in the PSM:

> The Government has determined 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 interests of third parties who deal with the Government.[27]

The Commission's views

4.19 The ALRC's current view is that most of the content of the PSM—the 'lead policy statement on protective security for the Commonwealth'[28]—should be placed in the public domain. This information is not only of interest to government departments, agencies and contractors. Other parties, including the media, freedom of information applicants and the general public, have a legitimate interest in knowing how and why government information and other public assets are classified and protected, and where responsibility for protective security measures falls. It would also increase awareness of the PSM and its contents both within and outside government including, for example, among officers and staff of courts and tribunals. Increased understanding of the need to protect classified and security sensitive information is likely to assist in preventing the unnecessary disclosure of such information.

4.20 Placing most of the PSM in the public domain would not require disclosure of genuinely sensitive protective security information. As with ACSI 33, this level of information could be included in separate documents that were appropriately classified and protected.

---

26 The Cabinet Office (UK), *Correspondence*, 4 October 2003.

27 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 5, [1.4]. See the further discussion of the principles of open government in Ch 3.

28 Attorney-General's Department, *Protective Security Coordination Centre Home Page*, <www.ag.gov.au/www/protectivesecurityhome.nsf> at 29 August 2003.

Proposal 4–1 A revised Australian Government Protective Security Manual should be placed in the public domain, with any sensitive protective security information removed.

Proposal 4–2 Sensitive protective security information that is relevant across the whole of government, or relevant to any particular Australian Government agency, should be included in a separate document or documents. These documents should be classified in accordance with the standards currently set out in the *Commonwealth Protective Security Manual.*

Classifying information in accordance with the PSM

4.21 The Australian Government's stated policy is to keep security classified information to the necessary minimum.[29] The PSM notes that over-classification is undesirable for the following reasons:

- it unnecessarily limits public access to government information;
- it imposes unnecessary, costly administrative arrangements that may remain in force for the life of the document, including repository arrangements for records transferred to the National Archives of Australia (NAA);
- the volume of security classified information may become too large for an agency to protect adequately; and
- classification and security procedures may be brought into disrepute if the classification is unwarranted. This may lead to classifications and protective markings in general being devalued or ignored by agency employees or receiving agencies.[30]

4.22 The Australian National Audit Office (ANAO) provides independent audit advice to agencies by undertaking performance and financial statement audits. As part of its normal auditing function, ANAO has established a program to audit protective security arrangements within agencies.[31] In a 1999 Audit Report on six government agencies holding classified, including national security classified, information,[32] ANAO noted that:

29 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 28, [6.20].
30 Ibid, C 34, [6.44].
31 Ibid, A 22, [6.4], [6.6].
32 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999).

> All organisations incorrectly classified files with over-classification being the most common occurrence.[33]

4.23 The ANAO recommended that these organisations implement procedures and conduct staff training to assist in ensuring the proper application of the classification system. For security reasons, the organisations themselves were not named in the report, but it is of concern that three were described as holding 'a range of national security and non-national security information at all classification levels'.[34]

4.24 The PSM states that the person responsible for classifying information is the person responsible for preparing it ('the originator') or 'actioning' it if it is generated outside Australia.[35] The originator is required to assess the consequences that would flow from the unauthorised disclosure or misuse of official information, and to decide whether the information should be security classified. In relation to information created outside Australia, this decision is made on receipt of the information and should be consistent with the provisions of any bilateral treaty concerning the protection of classified information in force between Australia and the country generating the material.[36]

4.25 The PSM does not expressly require a person who classifies information to hold a particular level of security clearance or that classification decisions are taken at a particular level of seniority. Advice provided to the ALRC indicates that this level of detail is left to stipulation in agency-level security policies and plans.[37] However, the PSM does require agencies to 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.[38] Agencies are also encouraged to have a procedure for confirming initial security classifications, especially if the classification is not normal or standard for that agency.[39]

4.26 The PSM makes clear that agencies should only classify information and maintain that classification when there is a clear and justifiable need to do so. The decision to classify should be based on the criteria set out in the PSM and not on any extraneous reason.[40]

4.27 The New Zealand manual, *Security in the Government Sector*, provides that only Chief Executives and heads of government departments and agencies have authority to classify material. While they may delegate that authority to senior staff, the guidelines state that this should be done sparingly and that only appropriate senior staff should be

---

33 Ibid, [2.84].
34 Ibid, [1.11].
35 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 27, [6.14].
36 Bilateral treaties concerning the protection of classified information to which Australia is a party are discussed further in Ch 2.
37 Protective Security Coordination Centre, *Correspondence*, 23 September 2003.
38 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 26, [6.9].
39 Ibid, C 27, [6.16].
40 Ibid, C 10, [2.7].

given authority to classify material Secret or Top Secret.[41] In the United States, the authority to classify information rests with the President, the Vice President, agency heads and officials formally nominated by the President. This authority may be delegated, but only in limited circumstances. The delegation must be in writing and identify the official by name or position title.[42]

4.28 US Executive Order 12958 imposes sanctions on:

> Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees if they knowingly, willfully, or negligently ... classify or continue the classification of information in violation of this order or any implementing directive.[43]

4.29 Executive Order 12958 expressly prohibits the classification of information in order to:

> (1) conceal breaches of the law, inefficiency, or administrative error;
>
> (2) prevent embarrassment to a person, organization, or agency;
>
> (3) restrain competition; or
>
> (4) prevent or delay the release of information that does not require protection in the interest of the national security.[44]

Consultations and submissions

4.30 The submissions of both the Attorney-General's Department and the Australian Press Council expressed support for a stronger statement by the Australian Government in relation to classifying information for inappropriate or insufficient reasons.[45] The Attorney-General's Department suggested that:

> As a means of reinforcing the correct purposes for applying a security classification, the PSM could prohibit applying a security classification for certain purposes. A possible example would be a standard that prohibits the use of a security classification to frustrate otherwise lawful access to information.[46]

4.31 The Press Council favoured a provision along the lines of the provision found in US Executive Order 12958, and it noted that:

---

41 Department of the Prime Minister and Cabinet (NZ), *Security in the Government Sector* (2002), 3–4.
42 *Executive Order 12958—Classified National Security Information*, 17 April 1995, s 1.3.
43 Ibid, s 5.5.
44 Ibid, s 1.7(a).
45 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003; Australian Press Council, *Submission CSSI 17*, 5 December 2003.
46 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

> It would like to see the Commonwealth government introduce reforms which would protect the rights of the Australian public to have access to government information, by placing an onus on government officers to classify information appropriately.[47]

The Commission's views

4.32 The ALRC has not received information expressly indicating that the existing guidelines in the PSM on how and by whom information is classified are inadequate. However, the ANAO report suggested that agencies incorrectly classify a significant amount of information.[48] More detailed guidance is provided on this issue in documents equivalent to the PSM in other jurisdictions. In New Zealand and the United States, for example, the authority to classify information formally resides at a very senior level and guidelines are provided in relation to the delegation of that authority. In the US, in particular, the decision to classify information is treated as a very serious one, with penalties potentially imposed on decision makers who classify information for inappropriate reasons.

4.33 It would appear consistent with the Australian Government's policy approach to the classification of information that classification decisions are taken at a sufficiently senior level to ensure that only that information which genuinely requires protection is classified. This may not always be the 'originator' of the document, although the originator is likely to be involved in the decision to refer information to an officer authorised to classify information. In these circumstances, the originator would be required to articulate why the information should be considered for classification rather than simply assigning a classification in the ordinary course of business. This is likely to lead to a more considered approach to classification decisions. In addition, if the decision to classify is taken at an appropriately senior level, this should eliminate the need for the classification decision to be confirmed, as is currently recommended by the PSM.[49]

4.34 The ALRC's preliminary view is that the PSM (revised as discussed above and placed in the public domain) should be amended to ensure that information is classified by an experienced officer, at the appropriate level. This may not be the 'originator' of the information in every case. It would also seem sensible that officers authorised to classify information should hold requisitely high security clearances.

4.35 While there are a number of statements in the PSM indicating that agencies should only classify information when there is a clear and justifiable need to do so and that the decision to classify should be based on the criteria set out in the PSM and not on any extraneous reason, this principle is not expressly included in the list of minimum standards set out in Part C of the PSM. The ALRC believes that this principle should be given more prominence and expressly included in the list of minimum

---

47 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

48 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), 40.

49 See [4.25] above.

standards. It may also be useful to include examples in the text of the PSM of what would amount to 'extraneous reasons', such as those set out in s 1.7(a) of US Executive Order 12958.[50] The reason set out in s 1.7(a)(4)—to 'prevent or delay the release of information that does not require protection in the interest of the national security'—would cover the example provided in the submission by the Attorney-General's Department.[51]

4.36 In the US, classifying information in contravention of s 1.7(a) of Executive Order 12958 has the potential to attract disciplinary sanctions. The extent to which the minimum standards set out in the PSM are, or might be made, enforceable, for example, through the APS Code of Conduct, is discussed further below.[52] One effect of making the minimum standards enforceable would be that officers who classified information for inappropriate reasons would become subject to disciplinary action.

Proposal 4–3 The revised Australian Government Protective Security Manual should be amended to provide further and more explicit guidance about who is authorised to classify information. In particular, it should ensure that information is classified by an experienced officer of appropriately high seniority and holding an appropriately high security clearance.

Proposal 4–4 The minimum standards in the revised Australian Government Protective Security Manual should be amended to include an express statement that: (a) information should only be classified when there is a clear and justifiable need to do so; and (b) the decision to classify should be based on the criteria set out in the Protective Security Manual and not on any extraneous reason.

Reclassifying and declassifying information

4.37 To keep the volume of security classified information to the necessary minimum, the PSM encourages agencies to limit the duration of classification and to establish review procedures,[53] although the PSM does not provide detailed guidance on the proposed procedures.

4.38 The PSM notes that, in assigning a classification, agencies should consider whether it is possible to place a time limit on the classification. This is one way information can be declassified, or its classification downgraded, in appropriate circumstances when the passage of time has removed or reduced the sensitivity that originally attached to the material. If this is not done, other agencies sharing the information and

50 See [4.28] above.
51 See [4.30] above.
52 Commencing at [4.92] below.
53 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 34, [6.45].

the National Archives of Australia (NAA) must continue to treat the information as classified, even where such protection is no longer necessary. The ANAO noted in its Report:

> There was no evidence among the papers examined of time limited protective markings. No organisation seemed to have given any consideration to such classifications, despite a common view from many respondents that much of the information was only sensitive for short time periods prior to becoming public.[54]

4.39 The ANAO recommended the use of time-limited classifications.

4.40 While it is relatively straightforward to set a time limit in relation to some material (for example, Budget documents that require protection until their public release), this may prove to be more difficult in relation to national security information. As the PSM notes, it is important that the classifying officer is confident that on the specified date the information will no longer need protection. In relation to national security information, it is likely that scheduled or regular reviews of classification will more safely and accurately identify documents that can be declassified or given a lower classification. The PSM provides that only the agency that assigned the original classification is permitted to reclassify or declassify information and so it is the originating agency that would be responsible for conducting any such review.

4.41 The PSM does not provide any detail in relation to the proposed review procedures but 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'.[55] The PSM also encourages recipients of information to challenge any security classification they believe is inaccurate.[56]

4.42 Under the *Archives Act 1983* (Cth), the NAA is responsible for providing public access to government records that are more than 30 years old. The NAA encourages agencies to declassify records, wherever possible, before transferring them to the NAA although the NAA advises that this rarely occurs in practice.[57] Where classified records are transferred to the NAA, they retain their classification and are stored and handled accordingly. Under the *Archives Act*, the NAA may exempt documents from public access on a range of grounds including on the basis that release of the document would damage security, defence or international relations.[58] However, the fact that a record is classified does not mean that it is automatically exempt, and all records are assessed on

---

54 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), [2.93].
55 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 35, [6.49].
56 Ibid, C 35, [6.50].
57 National Archives of Australia, *Correspondence*, 1 October 2003.
58 *Archives Act 1983* (Cth), s 33(1).

a case-by-case basis. Where a security classified record is released under the Act, the classification ceases to have effect.[59]

4.43 The Canadian *Security Organisation and Administration Standard* and the New Zealand security manual provide more detailed guidance in relation to such reviews. For example, the New Zealand manual provides that:

> Organisations should institute systems of review for downgrading classified material. This especially applies to material in current use. The security instructions for material should include details about downgrading ...
>
> [Organisations should] consider the following steps:
>
> - automatically downgrade information that becomes generally known after an event such as operations, moves, conferences, constitutional changes or visits
> - review accumulated material for downgrade, or destroy surplus material that is not required for records, after an operation or sequence of events
> - review files, media and contents for regrading when they are taken out of or brought back into current use
> - review accountable documents for regrading when they are mustered for periodical checks
> - review technical or scientific reports for regrading when they are over five years old, or some other specified period.[60]

4.44 The New Zealand manual also suggests that classified material be endorsed with the date on which the classification is to be reviewed.[61]

4.45 The relevant Canadian Standard provides that agencies should apply an automatic expiry period of 10 years where material is classified Confidential or Secret. This rule does not apply to information classified Top Secret, information received from foreign governments or cabinet documents. The Standard notes that:

> The risks associated with the use of an automatic expiry date are acceptable because removing material from the classification scheme is not synonymous with making it publicly available. The normal access application review process would still apply.[62]

4.46 Canadian agencies are empowered to declassify or downgrade information from other agencies following consultation with the relevant agency, where this is possible. Agencies are required to review the classification of information following a request for access under the *Access to Information Act 1985* or the *Privacy Act 1985* and are

---

59 Ibid, s 59.
60 Department of the Prime Minister and Cabinet (NZ), *Security in the Government Sector* (2002), 3–6.
61 Ibid, 3–21.
62 Treasury Board of Canada Secretariat, *Security Organization and Administration Standard 2–01*, 1 June 1995, [12.2].

required to develop agreements with the National Archives of Canada to declassify or downgrade sensitive information transferred to the control of the Archives. The Standard makes clear that information is to remain classified only for the time it requires protection, after which it is to be declassified or its classification downgraded. Agencies are to encourage originators and users of sensitive information to review its sensitivity on a continuing basis, and agency guidelines are required to specifically confer authority to declassify or downgrade information.[63]

4.47 Part 3 of US Executive Order 12958, which deals with declassification and downgrading of classification, is very clear on this point:

> Information shall be declassified as soon as it no longer meets the standards for classification under this order.[64]

4.48 As noted above, the Executive Order imposes sanctions on:

> Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees if they knowingly, willfully, or negligently ... continue the classification of information in violation of this order or any implementing directive.[65]

4.49 The Executive Order also provides that, at the time of original classification, the classifying authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. If this is not possible, information is to be marked for declassification 10 years from the date of the original decision unless the classifying authority determines that the sensitivity of the information requires that it remain classified for up to 25 years.[66] Classified information must be marked with declassification instructions.[67]

4.50 Classified records that are more than 25 years old and have been determined to have permanent historical value are automatically declassified whether or not the records have been reviewed. Agency heads may exempt particular documents from automatic declassification on certain specified grounds; for example, that they would reveal information that would 'seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities.'[68] Information exempted from automatic declassification remains subject to mandatory and systematic declassification reviews.

4.51 Holders of classified information who 'in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification of

---

63 Ibid, [12].
64 *Executive Order 12958—Classified National Security Information*, 17 April 1995, s 3.1(a).
65 Ibid, s 5.5. See [4.28] above.
66 Ibid, s 1.5.
67 Ibid, s 1.6.
68 Ibid, s 3.3.

the information in accordance with agency procedures.'[69] In addition, the Director of the Information Security Oversight Office (ISOO), a division of the National Archives and Records Administration (NARA), may require that information be declassified. Decisions by the Director of ISOO may be appealed to the President.

4.52 ISOO is responsible for oversight of the national security classification programs in over sixty US government entities. The Office has a range of responsibilities including the conduct of on-site inspections and reviews to monitor agency compliance with classification and declassification programs, the development of security education material, and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).

4.53 ISCAP was established by Executive Order 12958[70] and comprises six members representing the Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs. ISCAP has three main functions:

- to decide on appeals where authorised holders of information have challenged the classification of that information and the challenge has been rejected at agency level;

- to approve, deny or amend agency exemptions from automatic declassification; and

- to decide on appeals by members of the public who have requested that information be declassified and whose requests have been rejected at agency level.[71]

4.54 Most of ISCAP's work involves considering appeals from members of the public. ISCAP's decisions are made by voting and a majority is required to overturn an agency decision. In 2002, ISCAP made decisions in relation to 101 documents in 37 separate appeals—it voted to declassify 11 of these documents (11%) in full, to declassify parts of 56 documents (55%) and to affirm agency decisions in relation to 34 documents (34%). Between May 1996 and December 2002, ISCAP declassified information in 76% of the documents it considered. ISCAP reports that in this period there was a marked decrease in the number of documents that came before it for consideration and that this is attributable to agencies declassifying more of the information they process in accordance with Executive Order 12958.[72]

---

69 Ibid, s 1.8.
70 Ibid, s 5.3.
71 Ibid, s 5.3(b).
72 US National Archives and Records Administration, *Highlights of Activities of the Interagency Security Classification Appeals Panel January–December 2002* (2003).

4.55 It is unclear to what extent Australian government agencies implement the provisions of the PSM in relation to review of classification. In 1980, Mason J commented in one High Court decision that:

> Security classification is given to a document when it is brought into existence. Thereafter, it seems, there is no regular procedure for reconsidering the classification of documents, with the consequence that the initial classification lingers on long after the document has ceased to be a security risk. My impression is that, with one exception, the documents have not been reconsidered for classification since they were brought into existence.[73]

4.56 More recently, the ANAO reported that, in relation to the six government agencies reviewed:

> There was no established program for reviewing the classification of files. In addition, where re-classifications did occur, no records were maintained.[74]

4.57 The ANAO recommended that organisations develop formal security monitoring and review programs including periodic review of file classifications.[75]

Consultations and submissions

4.58 The Australian Press Council submitted that:

> The difficulty with the classifications set down in the PSM is that, being subjective, they rely on the discretion of government officers to make appropriate and judicious decisions as to which items should be classified and the level of classification ... there may be a tendency of government officers to restrict access to information in order to limit scrutiny and thereby avoid criticism for inefficiency or incompetence.
>
> The characteristics of the classification scheme—its breadth of scope and the subjectivity of its definitions—provide enormous potential for abuse.[76]

4.59 In order to counter these potential problems, the Press Council supports the establishment of clear mechanisms to review classifications including an independent body to conduct such reviews. In addition, the Press Council suggests the need for a mechanism to allow the media and the public to identify that classified documents exist, without revealing the sensitive contents of such documents. This is on the basis that:

> Any review process will be ineffective if the media have no way of knowing that classified information exists.[77]

---

73 *Commonwealth v Fairfax* (1980) 147 CLR 39, 53.
74 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), [2.111].
75 Ibid, [2.115].
76 Australian Press Council, *Submission CSSI 17*, 5 December 2003.
77 Ibid.

4.60 The Australian Crime Commission (ACC) also submitted that the classification process involved a certain amount of subjectivity and that the way the process was handled varied from agency to agency. The ACC suggested that:

> an effective regime of training by agencies of those originating and handling security classified information will enable the security classification process to be properly used. The Agency Security Advisor, and not an independent panel, is the best point for reviewing security classification decisions and disputed calls, which cannot be readily resolved by reference to the PSM, and may need to be subjected to a formal risk assessment process.[78]

4.61 The Attorney-General's Department did not support the establishment of an independent body to review classifications, stating that:

> Only the source agency or department can appropriately classify security information. The source agency or department will have the knowledge and experience to assess the sensitivity of the information in context. An independent body will not have such knowledge. Requiring agencies and departments to defend the classification they have assigned to information before such a body is an impractical suggestion. If an independent body could overturn the classification of the source agency or department, certainty and consistency would be removed from the classification process.[79]

The Commission's views

4.62 Existing Australian Government policy seeks to limit the amount of information that is classified and suggests that, where documents are classified, review mechanisms should be put in place to reclassify or declassify documents no longer needing the same level of protection. However, the ANAO Report indicates that this is not occurring as a matter of general practice, at least in the six agencies reviewed, and that a great deal of information remains over-classified. For the reasons set out above,[80] this is not good administrative practice and may contribute to a culture in which classified information is not adequately protected.

4.63 As noted above, in Canada and the US classified information (with some exceptions) is automatically declassified after a specified period—10 years in Canada and 25 years in the US—even if no review action is taken. In New Zealand and Australia, however, the default position is different. Material remains classified if no review action is taken. In the absence of appropriate review mechanisms, this has the potential to undermine government policies in relation to the protection of classified and security sensitive information. Mason J's comments in *Fairfax* give some indication of the impact that this may have on the attitude of courts and tribunals to the classification system as a whole.

4.64 The ALRC proposes that Australia move to a system with two elements that encourage the proper declassification and reclassification of sensitive material:

---

78 Australian Crime Commission, *Submission CSSI 15*, 13 October 2003.
79 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
80 See [4.21] above.

(a) classified and security sensitive information should be reviewed with a view to declassification or reclassification in a number of specified circumstances:

(i) when it is first classified (which may become unnecessary if Proposal 4–3 is adopted);

(ii) before transfer to the National Archives of Australia (NAA), in order to reduce the volume of archived material held by the NAA that remains unnecessarily classified;

(iii) in response to any challenge to its classification status (for example, by recipients of information, as suggested in the PSM);[81] and

(iv) when there is any need or proposal to use that information in a public forum such as in court or tribunal proceedings, or in response to a freedom of information application.

(b) automatic declassification 30 years after receipt or creation, to coincide with the period that applies to the release of government papers under the *Archives Act 1983* (Cth),[82] unless a review done at that time concludes that the material should remain classified for a further period of up to five years. These reviews should continue at five-year intervals.

4.65 However, classifying agencies should be at liberty to give any item of classified material an earlier date by which the material should be reviewed for reclassification or declassification.

4.66 Government agencies should be required to establish and enforce procedures to ensure that classified information held by them is regularly reviewed in accordance with these principles. This would require the application of some resources, but is consistent with existing government policy and will help to ensure that only that information which continues to require protection remains classified.

4.67 The ALRC assumes that an informal re-assessment of the classification status of any classified material is already done when considering freedom of information applications or the use of classified or security sensitive information in court. Before making an application to a court for public interest immunity, the relevant government officers and their lawyers would presumably consider carefully the extent to which any such material can be disclosed in court without undermining Australia's defence or security. Although that exercise is not necessarily done with a view to a formal reclassification or declassification, it would seem that much the same work would be

81 See [4.41] above.
82 See [4.42] above.

required—all that remains to do would be the formal process of reclassification or declassification.

4.68 The ALRC also considers that a range of mechanisms in use in other jurisdictions could be adopted in Australia as part of standard review procedures without imposing significant extra costs, including:

- endorsing classified material with a date on or by which the classification is to be reviewed; and

- developing agreements with the NAA to declassify or downgrade sensitive information transferred to its control. However, these would be absorbed into any reforms in line with those suggested in [4.64] above: see Proposal 4–5.

4.69 The ALRC notes the Australian Press Council's support for the establishment of an independent inter-agency review panel to review classifications along the lines of ISCAP in the US. The Attorney-General's Department submitted that only source agencies have the knowledge and experience to assess the sensitivity of classified information in context and that an independent body would not be able to do this effectively.[83] However, in the US, ISCAP members are drawn from senior levels in agencies that regularly handle such information. The ALRC considers that a body of this kind could properly consider these issues on the basis of advice from the source agency, and it is entirely appropriate that agencies be able to defend the classifications they assign to information.

4.70 Accordingly, the ALRC proposes that such a body be established in Australia along the lines of ISCAP. The ALRC notes that the Administrative Appeals Tribunal (AAT) has power to review decisions by some agencies and Ministers to refuse access to classified or security sensitive documents under the *Freedom of Information Act 1982* (Cth), although the intelligence agencies are generally exempt from the coverage of that Act. The AAT's power is also somewhat limited in relation to documents affecting national security, defence or international relations.[84] Some consideration should be given to the way in which the jurisdiction of the proposed inter-agency review panel and that of the AAT are established so that there are clear lines of appeal governing classified and security sensitive information and no unnecessary overlap.

83 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
84 This issue is discussed in Ch 3.

Proposal 4–5 The Australian Government should adopt a system of declassifying and reclassifying sensitive material with two elements:

(a) classified and security sensitive information should be reviewed with a view to declassification or reclassification in a number of specified circumstances:

  (i) when it is first classified (which may become unnecessary if Proposal 4–3 is adopted);

  (ii) before transfer to the National Archives of Australia (NAA), in order to reduce the volume of archived material held by the NAA that remains unnecessarily classified;

  (iii) in response to any challenge to its classification status (for example, by recipients of information, as suggested in the *Commonwealth Protective Security Manual*); and

  (iv) when there is any need or proposal to use that information in a public forum such as in court or tribunal proceedings, or in response to a freedom of information application.

(b) automatic declassification 30 years after receipt or creation, to coincide with the period that applies to the release of government papers under the *Archives Act 1983* (Cth), unless a review done at that time concludes that the material should remain classified for a further period of up to five years. These reviews should continue at five-year intervals.

However, classifying agencies should be at liberty to give any item of classified material an earlier date by which the material should be reviewed for reclassification or declassification.

Proposal 4–6 The Australian Government should establish an independent administrative body to review classification decisions, along the lines of the US Interagency Security Classification Appeals Panel.

Monitoring agency compliance with the PSM

4.71 There are a number of existing mechanisms in place to monitor the performance of Australian government agencies, including in relation to compliance with the minimum standards in the PSM. While the ALRC has not received any information expressly indicating that the standards in the PSM are inappropriate or inadequate,

there is some evidence that agencies are not implementing the standards in a comprehensive or consistent way.[85] More recent reports in relation to the intelligence agencies indicate that there has been some improvement in protective security performance in recent years,[86] but it is difficult to know whether this is the case across the public service more generally, as the results of the PSCC service-wide annual survey on protective security are not made public.[87]

4.72 As noted above, the ANAO performs audits of the protective security arrangements within government agencies to assess how well agencies are managing their protective security policies and procedures. Under s 32 and 33 of the *Auditor-General Act 1997* (Cth), agencies are required to provide documents, information and access to premises to allow the ANAO to conduct such audits. The audit reports are public documents. However, the audits are not conducted at frequent or regular intervals in relation to any individual agency.

4.73 In 1999, the Inspector-General of Intelligence and Security (IGIS) conducted a review of security procedures following the arrest in the United States of a former DIO employee, Jean-Philippe Wispelaere, on charges of attempting to sell highly classified material. The Inspector-General provided a confidential report to the Australian Government making over 50 recommendations to improve security in departments that handle highly classified material and Australia's intelligence and security agencies.[88]

4.74 As discussed above in Chapter 2, the Parliamentary Joint Committee on ASIO, ASIS and the DSD conducted its own inquiry into these issues and tabled its report, *Private Review of Agency Security Arrangements*,[89] in Parliament on 13 October 2003.[90] That report states:

> In general, the Committee found that protective security arrangements within the three agencies were sound, and in most respects, exceeded the standards required by the PSM. The Committee found further that each of the agencies had made impressive progress in implementing the recommendations of the IGIS Inquiry.[91]

4.75 As part of the Government response to the Inspector-General's report, the PSCC now conducts an annual protective security survey of Australian Government agencies. The survey is designed to measure the extent of agency compliance with the PSM minimum standards. The initial survey was sent to over 130 Australian Government

---

85 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999).

86 Parliamentary Joint Committee on ASIO ASIS and DSD, *Private Review of Agency Security Arrangements* (2003).

87 See [4.75] below.

88 The Hon Daryl Williams AM QC MP, *Improving Security Within Government*, News Release, 21 September 2000.

89 Parliamentary Joint Committee on ASIO ASIS and DSD, *Private Review of Agency Security Arrangements* (2003).

90 See [2.43] above.

91 Parliamentary Joint Committee on ASIO ASIS and DSD, *Private Review of Agency Security Arrangements* (2003), viii.

agencies.[92] In the following year, the survey was sent to 190 agencies.[93] While the report to Government on the results of the survey was not made public, the ANAO noted in its report *Physical Security Arrangements in Commonwealth Agencies* that:

> Overall, the [PSCC] report identified that the status of physical security was generally sound. However, deficiencies were noted in the agencies' application of the complementary measures of personnel security and/or information security. Complacency was identified as an issue in some agencies. In others, there was a lack of commitment to structured processes and practices. In addition, there was generally a low level of understanding of the minimum standards of the PSM.[94]

4.76 The Attorney-General's Department *Annual Report 2002-03* noted that:

> [The survey] found that the status of protective security across all Commonwealth agencies appears inconsistent. Comparison between the 2001 and 2002 survey results shows some areas of protective security have improved, others remain unchanged, and some have declined.[95]

4.77 The *Public Service Act 1999* (Cth) provides the legal framework for employment in, and management of, the Australian Public Service (APS) and includes the APS Values and Code of Conduct discussed below at [4.96]–[4.110].[96] The *Public Service Act* applies to all APS employees and Agency Heads but, significantly, officers of ASIO and ASIS are not employed under the provisions of the Act.

4.78 The Act sets out the functions of the Public Service Commissioner, which include:

- evaluating the extent to which agencies incorporate and uphold the APS Values; and
- evaluating the adequacy of systems and procedures in agencies for ensuring compliance with the Code of Conduct.[97]

4.79 Under s 44 of the Act, the Public Service Commissioner is required to prepare a report to the Prime Minister, for presentation to Parliament, on the state of the APS during the preceding financial year. Every year the APS Commission sends a questionnaire to each agency (the Agency Questionnaire) seeking information on which to base the report. Under s 44(3), Agency Heads are required to provide the Commissioner with the information needed to prepare the report. The State of the Service Report for

---

92 Attorney-General's Department, *Annual Report 2001–02* (2002).
93 Attorney-General's Department, *Annual Report 2002–03* (2003).
94 Australian National Audit Office, *Physical Security Arrangements in Commonwealth Agencies*, Report 23 (2002–2003), 31, [1.22].
95 Attorney-General's Department, *Annual Report 2002–03* (2003).
96 The Australian Public Service Values and Code of Conduct are set out in full in Appendix 3.
97 *Public Service Act 1999* (Cth), s 41(1)(a) and (b).

2001–02 examined the measures agencies are using to prevent unauthorised disclosure, noting that:

> The leaking of information cannot be controlled and discouraged solely through measures designed to enforce compliance. For the 43% of agencies that do not periodically remind their employees of their obligations, more work is required.[98]

4.80 In addition, the PSM recommends that agencies conduct regular internal security audits to ensure that protective security measures are being implemented efficiently and effectively.[99]

The Commission's views

4.81 A range of mechanisms exists to monitor agency compliance with protective security procedures in relation to classified and security sensitive information. Some of these mechanisms potentially involve the exercise of compulsory powers—for example, audits by the ANAO, inquiries by the Joint Parliamentary Committee and reports by the Public Service Commissioner. Others rely on voluntary co-operation from agencies such as the annual protective security survey by the PSCC. Some of the mechanisms cover *Public Service Act* agencies as well as the intelligence agencies, some are more limited. For example, as noted above,[100] the Public Service Commissioner does not have jurisdiction in relation to ASIO and ASIS.

4.82 The ALRC's current view is that, despite the number of existing review mechanisms, there are gaps in terms of regularity, publicity and feedback that mean that the mechanisms may not be working in a sufficiently active way to encourage continuous improvement in agency performance.

4.83 ANAO audits are conducted on an independent and mandatory basis and the results of the reports are made public. This means that all agencies may access the reports and make use of the lessons learnt, both positive and negative, from the experiences of other agencies. ANAO does not, however, conduct protective security audits of every agency on a regular basis and it is unclear to what extent agencies actually take note of and act upon ANAO reports in relation to other agencies.

4.84 The PSCC's annual protective security survey is intended to target all agencies on a regular basis. The collection of the information is by means of a self-reporting survey. Unlike the Joint Parliamentary Committee, ANAO, the Inspector-General of Intelligence and Security and the APS Commissioner, the PSCC does not have express legislative authority to require agencies to participate in the survey and does not have authority to access premises and information independently. While the survey results are analysed by PSCC and a report submitted to the Government, the report is not made public and there does not appear to be a formal mechanism for providing feed-

98 Australian Public Service Commission, *State of the Service Report 2001–2002* (2002), 29.
99 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), A 22, [6.1].
100 See [4.77] above.

back and advice to agencies on the survey results. This is likely to limit the extent to which the information collected is used as the basis for improving performance in individual agencies although it may inform and help to target the general protective security training provided by the PSCC.

4.85 The APS Commission Agency Questionnaire targets all *Public Service Act* agencies on a regular basis and participation in the survey is mandatory. The results of the survey are made public in the annual State of the Service report. To date, the Agency Questionnaire has not consistently and comprehensively addressed protective security standards but has focussed on particular issues each year such as the unauthorised disclosure of official information in the 2001–2002 Report and record keeping more generally in 2002–2003.

4.86 It remains unclear to what extent agencies comply with the PSM recommendation to conduct regular internal protective security audits.

4.87 Elements of these various mechanisms could be combined and improved to ensure that agency compliance with the PSM minimum standards is more effectively monitored, that the results of the monitoring are shared among agencies and made public (to the extent that this is appropriate) and that agencies receive feedback and advice on an individual level.

4.88 The Agency Questionnaire could be expanded to include a section seeking information on agency compliance with protective security standards, developed in consultation with the PSCC and, possibly, the ANAO, and based closely on the existing PSCC protective security survey. Combining these two processes would avoid unnecessary duplication.

4.89 To the extent appropriate, the results of the Agency Questionnaire should be made public in the annual State of the Service Report. This part of the report could be developed in consultation with PSCC. In addition, it would be valuable if the PSCC were to scrutinise survey responses with a view to providing agencies with specific advice on improving protective security performance.

4.90 The Inspector-General of Intelligence and Security would also need to be involved in relation to the intelligence agencies not subject to the jurisdiction of the APS Commissioner.

4.91 Agencies should be encouraged to align internal security auditing procedures with these processes so that the information collected as part of the internal audit can be used to respond to the protective security questions in the annual Agency Questionnaire.

Proposal 4–7 The Australian Public Service Commission Agency Questionnaire should be expanded to include a section seeking information on agency compliance with protective security standards in relation to the handling of classified and security sensitive information. To the extent appropriate, the results of this section of the Australian Public Service Commission Agency Questionnaire should be included in the annual State of the Service Report to the Prime Minister.

Proposal 4–8 The Inspector-General of Intelligence and Security should seek information on agency compliance with protective security standards in relation to the handling of classified and security sensitive information from the intelligence agencies not subject to the jurisdiction of the Australian Public Service Commissioner. The results should be included in an annual report to the Prime Minister.

Proposal 4–9 The Protective Security Coordination Centre should scrutinise agency responses to the questionnaires and enquiries referred to in Proposals 4–7 and 4–8 with a view to providing agencies with specific advice on improving protective security performance.

Proposal 4–10 Government agencies should be encouraged to schedule internal security auditing procedures so that information collected as part of the internal audit can be used to respond to the annual questionnaires from the Australian Public Service Commission and the Inspector-General of Intelligence and Security.

Enforcing the standards in the PSM

4.92 The Terms of Reference for this Inquiry specifically ask the ALRC to examine whether the protective security standards set out in the PSM are enforceable. The standards in the PSM are provided for the guidance of Australian Government agencies and officers, and for contractors and their employees who perform services for or on behalf of the Australian Government. They are designed to ensure that government functions are carried out in an appropriate security environment and that government information receives adequate protection.

4.93 There are a number of statements within the PSM that the standards are not legally enforceable *per se*. 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.[101]
>
> 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.[102]

4.94 These statements indicate that the Government considers that the standards are mandatory in some sense and that there is a link between the standards and legislative requirements for protecting official information. The PSM notes that mandatory minimum standards are indicated by the use of the term 'must'. The use of the term 'must' is in contrast to other terms used in the manual such as 'should', 'strongly recommended' and 'are advised to'.[103]

4.95 There are a number of ways that the standards could be enforced indirectly:

- a breach of the standards could constitute a breach of the APS Code of Conduct;
- a breach of the standards could constitute a breach of contract; and
- a breach of the standards could constitute a breach of the criminal law governing the handling of official information such as the *Crimes Act 1914* (Cth) or the *Criminal Code Act 1995* (Cth). This issue, and other legal mechanisms available to prevent or punish unauthorised disclosures of official information, is discussed in Chapter 5.

Breach of APS Code of Conduct

4.96 Section 13 of the *Public Service Act* sets out the APS Code of Conduct, which binds APS employees, Agency Heads and statutory office holders.[104] The Code of Conduct provides in part that:

- an APS employee must behave honestly and with integrity in the course of APS employment;[105]
- an APS employee must act with care and diligence in the course of APS employment;[106]

---

101 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), A 18, [5.1].
102 Ibid, C 19, [4.17].
103 Ibid, A 18, [5.1].
104 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'.
105 Ibid, s 13(1).
106 Ibid, s 13(2).

- an APS employee, when acting in the course of APS employment, must comply with all applicable Australian laws;[107]

- 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;[108]

- an APS employee must maintain appropriate confidentiality about dealings that the employee has with any Minister or Minister's member of staff;[109]

- an APS employee must use Commonwealth resources in a proper manner;[110]

- an APS employee must not make improper use of:

  (a) inside information; or

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

  in order to gain, or seek to gain, a benefit or advantage for the employee or for any other person;[111]

- an APS employee must at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS;[112]

- an APS employee must comply with any other conduct requirement that is prescribed by the regulations.[113]

4.97 In some circumstances, a breach of the minimum standards in the PSM may constitute a breach of the APS Code of Conduct. For example, where an Agency Head has directed staff of the agency to adhere to those standards, a failure to comply could also constitute a breach of s 13(5). A failure to handle official information with due care would be inconsistent with the principles of effective information security practice set out in the PSM.[114] In some circumstances, this could also amount to a breach of s 13(2) or 13(8).

4.98 The PSM requires that only those who need to use or access official information to do their work should be given access to the information—commonly referred to as

---

107 Ibid, s 13(4).
108 Ibid, s 13(5).
109 Ibid, s 13(6).
110 Ibid, s 13(8).
111 Ibid, s 13(10).
112 Ibid, s 13(11).
113 Ibid, s 13(13).
114 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 9, [2.2].

the 'need-to-know principle'.[115] A breach of this principle may also contravene s 70 of the *Crimes Act 1914* (Cth) in some circumstances. Until recently, this might also have amounted to a breach of reg 2.1 of the *Public Service Regulations 1999* (Cth)—but a decision of the Federal Court in December 2003 has cast doubt on the validity of this provision.[116]

4.99 Regulation 2.1 of the *Public Service Regulations* provides:

> For the purposes of subsection 13(13) of the Act, an APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head's express authority, give or disclose, directly or indirectly, to any person any information about public business or anything of which the employee has official knowledge.

4.100 On 10 December 2003, Finn J of the Federal Court of Australia handed down a judgment that declared reg 7(13) of the *Public Service Regulations* invalid on the basis that it infringed the implied constitutional freedom of political communication. The substantive part of reg 2.1, set out above, is in identical terms to its predecessor, reg 7(13). The regulation was struck down on the basis that it failed the test of validity set out by the High Court in *Lange v Australian Broadcasting Corporation*[117] in that:

- it was a law that burdened the freedom of public servants to disseminate information and to make communications about government and political matters; and
- due to the breadth of the provision, it was not reasonably and appropriately adapted to serve a legitimate end the fulfilment of which is compatible with the maintenance of the system of government prescribed by the Constitution.

4.101 Finn J stated that:

> The difficulty in giving an affirmative answer to the second *Lange* question inheres in the 'catch-all' character of the regulation. One can identify readily enough some number of public interests or 'legitimate ends', both particular and general, which could be said to be comprehended by Reg 7(13) and which are compatible with the maintenance of the system of representative and responsible government. These range, for example, from national security and cabinet secrecy through privacy protection, to the maintenance of an impartial and effective public service in which the public can have confidence. But given the very generality of the regulation such legitimate end as may be served by it must itself be of an appropriately general character. For this reason the Commonwealth in its submissions relied upon the end of 'furthering the proper and efficient operation of the Government'. Subsumed within this was maintaining an orderly, efficient and disciplined public service. I emphasise the need for an end of a general character for this reason. Ends of a more particular character, for example,

---

115 Ibid, C 9, [2.4].

116 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433. This decision also has some relevance to s 70 of the *Crimes Act 1914*, which is discussed in Chapter 5.

117 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

> privacy protection or preserving Cabinet secrecy could reasonably be secured by greatly less burdensome and more precise and particular restrictions.[118]

4.102 This leaves open the possibility that a more focussed provision—in particular one expressly dealing with classified and security sensitive information—would be valid. Finn J acknowledged that:

> the State does have a legitimate interest in regulating the disclosure of official information by its officers and employees.[119]
>
> There are, unquestionably, species of official information the disclosure of which the State, properly, might wish to regulate or prohibit for reasons of public interest relating, variously, to the nature of the information, the circumstances of its generation or acquisition or the timing or possible consequences of its disclosure.[120]

4.103 It will now be necessary for the Australian Government to consider its response to this decision and any appeal from it.

4.104 The *Public Service Act* provides that an Agency Head may impose the following sanctions against employees who have been found 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.[121]

4.105 In addition, the *Public Service Regulations* 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.[122]

4.106 Basic procedural requirements for making a determination that an APS employee has breached the Code of Conduct are set out in the Public Service

---

118 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433, [80].
119 Ibid, [90].
120 Ibid, [100].
121 *Public Service Act 1999* (Cth), s 15(1).
122 *Public Service Regulations 1999* (Cth), reg 3.10.

Commissioner's Directions 1999, an instrument made under s 11(1) and 15(4) of the *Public Service Act*. An APS employee is entitled to seek review of an agency-level decision in all cases, except where the employee's employment has been terminated, by applying to the Merit Protection Commissioner.[123] Where an employee's employment has been terminated, the employee may seek redress under the *Workplace Relations Act 1996* (Cth). Employees also have the right to seek judicial review of the agency-level decision under the *Administrative Decisions (Judicial Review) Act 1977* (Cth).

4.107 Regulation 5.33 of the *Public Service Regulations* provides that:

> (1) The procedures used for a review conducted under this Division must meet the following minimum requirements:
>
> (a) the procedures must have due regard to procedural fairness;
>
> (b) the review must be conducted in private;
>
> (c) the review must be finished as quickly, and with as little formality, as a proper consideration of the matter allows.[124]

4.108 In 2002–03, the Merit Protection Commissioner received 43 applications for review of agency decisions in relation to breaches of the APS Code of Conduct.[125] Since the commencement of the Act, only one case considered by the Commissioner has concerned an employee sanctioned for releasing sensitive agency information. The case involved release of information to a newspaper journalist in breach of s 13(13) of the *Public Service Act* and reg 2.1 of the *Public Service Regulations*. The employee was reduced in classification and reassigned to other duties.[126]

4.109 Agency Heads are expressly bound by the Code of Conduct. The *Public Service Act* does not, however, specify the sanction for an Agency Head who breaches the Code of Conduct. The Public Service Commissioner is given power to inquire into alleged breaches of the Code of Conduct by Agency Heads and to report to the appropriate authority (usually the Prime Minister or other relevant Minister) on the results of such enquiries, including recommendations for sanctions where appropriate.[127]

4.110 The Public Service Commissioner's Directions make it clear that not all suspected breaches of the Code of Conduct need to be dealt with by way of determination.[128] Where a suspected breach appears to be minor, for example, it may be sufficient to counsel the employee about his or her conduct.

---

123 Ibid, reg 5.24.
124 Ibid, reg 5.33.
125 Australian Public Service Commission, *Public Service Commissioner Annual Report 2002–03* (2003), 110.
126 Merit Protection Commissioner, *Submission CSSI 10*, 29 August 2003.
127 *Public Service Act 1999* (Cth), s 41(1)(f).
128 *Public Service Commissioner's Directions 1999* (Cth), cl 5.1 note.

4.111 In contrast to the PSM, US Executive Order 12958 is *directly* enforceable. 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.[129]

Options for reform

4.112 While the protective security standards set out in the PSM are not enforceable *per se*, it is clear that there are significant links between the standards and the requirements of the APS Code of Conduct. The PSM states that the use of the term 'must' indicates mandatory minimum standards. In some circumstances a breach of those standards will also amount to a breach of the Code of Conduct. However, the extent to which this is so is not entirely clear.

---

129 *Executive Order 12958—Classified National Security Information*, 17 April 1995, s 5.5.

4.113 If it is intended that the minimum standards set out in the PSM are mandatory and enforceable (and it appears that this is the case in relation to some of the standards), this should be made absolutely clear. The current version of the PSM contains a great deal of general policy information and includes guidelines and recommendations that are neither precisely worded nor apparently intended to be binding. This has the potential to create uncertainty in relation to which of the standards in the PSM are mandatory and which are not. This is undesirable where breach of the mandatory standards can attract sanctions. The current document would benefit from some reworking to distinguish these separate elements. In particular, the ALRC proposes that those elements intended to be mandatory and to apply across government should be drawn together and clearly identified. The language of any such mandatory standards would have to be examined to ensure that it was clear and appropriate for provisions that had the potential to attract sanctions.

4.114 In its publication *Managing Breaches of the APS Code of Conduct*, the APS Commission states in relation to agency-specific codes of conduct:

> The misconduct procedures referred to in section 15(3) of the PS Act can be triggered only by a suspected breach of the Code of Conduct—as set out in the Act and Regulations. Agency-based codes, which may be useful in articulating expected conduct standards in that agency, cannot in themselves form the basis of misconduct action. If there is an infringement of an agency-based code, it will be necessary to link the conduct in question to a particular element in the APS Code of Conduct, if it is to form the basis of a misconduct process. It would be wise to link any provisions of agency-based codes to the APS Code in material that is distributed to staff.[130]

4.115 The same principles would apply to any government-wide standards that were intended to be mandatory for APS employees. In redrafting the mandatory standards as suggested above, it would be valuable to link the standards expressly to particular elements in the Code of Conduct, where possible.

4.116 This would not necessarily make such standards enforceable; however, there are a number of ways this could be achieved. Section 13 of the *Public Service Act* could be amended to add a new element to the Code of Conduct directed to ensuring that APS employees were required to comply with relevant protective security standards. Government-wide standards could be issued, for example, by the Attorney-General's Department. Agency-specific standards might also apply. Making a statement of this kind in the primary piece of legislation regulating APS employment would place a significant new emphasis on the issue of protective security. It would also ensure that mandatory protective security standards issued by the relevant authority were binding on APS employees and would make clear that a breach of those standards had the potential to attract sanctions.

---

130 Australian Public Service Commission, *Managing Breaches of the APS Code of Conduct* (2nd ed, 2002), 2.

4.117 As mentioned above, s 13(13) provides that APS employees must comply with any other conduct requirement that is prescribed by the regulations. Thus, an alternative option would be to amend the regulations to incorporate relevant protective security standards as additional conduct requirements. This has already occurred in relation to the duty not to disclose official information[131]—although, as noted above, the terms of the existing regulation have been found to be too broad.[132] Enacting the standards as regulations would give them the force of law and would make absolutely clear that these are binding and enforceable. While the disallowance procedure applying to regulations ensures that the operation of regulations is not delayed pending parliamentary approval, the process of amending the regulations would be more onerous than amending standards issued by the bureaucracy.[133]

4.118 A further alternative would be to ensure that Agency Heads, or other officers with authority to do so, expressly and clearly direct all agency employees to comply with the mandatory standards. The agency would then be in a better position to rely on s 13(5) to discipline officers in breach of those standards. This approach could be implemented immediately and without further legislative action, although the ALRC considers that this approach should only be pursued once the mandatory standards have been clearly identified and modified as necessary. This approach could also be adopted in relation to agency-specific guidelines and standards. In order to rely on s 13(5), the agency would need to demonstrate that the direction had been given by someone with authority to direct the employees and that the standards were lawful and reasonable.

4.119 One mechanism for reinforcing this process would be to require employees to sign a form acknowledging that they know and understand their obligations in relation to compliance with protective security standards. This mechanism is already in use in some agencies in relation to the unauthorised disclosure of official information.[134]

4.120 It would also be in the agency's and employee's interests to ensure that the standards were well understood, that employees were aware that the standards were mandatory and that breach of the standards could attract sanctions. The Australian Public Service Commission noted in its annual *State of the Service Report 2001–02* that, in relation to the APS Code of Conduct generally:

> Most agencies are taking steps to educate new employees about the Values and the Code. Nearly all agencies (94%) provide information on the Code of Conduct and the Values to new recruits in the course of induction training. There is however less effort

131 *Public Service Regulations 1999* (Cth), reg 2.1.

132 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433. See [4.100]–[4.103] above.

133 The *Acts Interpretation Act 1901* (Cth) provides that, generally, new regulations must be published in the *Gazette* and tabled in both Houses of Parliament within 15 sitting days of being made. The regulations may come into effect on a date specified, or on the date of publication in the *Gazette*, but remain subject to a notice of disallowance by either House of Parliament for 15 sitting days following tabling. Regulations cease to have effect if either House of Parliament passes a resolution disallowing the regulations, but they remain in force unless and until this happens.

134 Australian Public Service Commission, *State of the Service Report 2001–2002* (2002), 29.

> devoted to ensuring that a similar level of awareness exists among current employees. Many of the initiatives agencies use to promote an understanding of the Values and the Code to existing employees are passive in nature. For example, the majority of employees already employed in the APS can access the Code and the Values, as well as their agency's procedures for determining breaches of the Code, on their agency's Intranet. While this is a positive measure, the onus rests with employees to actively seek out and use the information ...
>
> In total, however, 40% of agencies provided their staff with no training in 2001–02, either mandatory or self-nominated, to ensure an understanding of the relevance of the Values and Code. A breakdown by size of agency reveals that 10% of large agencies, 43% of medium agencies and 50% of small agencies provided no such training.[135]

4.121 In relation to unauthorised disclosure of official information in particular, the report notes:

> Agencies report a range of measures to alert employees to their obligations not to release official information without authority, including through the induction process (used by 85% of agencies), promulgated policies (58%), CEIs [Chief Executive Instructions] (46%) and training programs (44%).
>
> A number of agencies commented that they require employees to sign a form on commencement of employment acknowledging their understanding of their obligations in regard to the disclosure of information. While the majority of employees are informed of their obligations in regard to official information on commencement, 42% of agencies reported that they do not provide employees with regular reminders of those obligations. By contrast, in some agencies, for example DFAT, the requirement to manage classified material in accordance with guidelines and avoid security breaches is reported to be an integral part of daily workplace culture, with staff reminded of their responsibilities regularly.[136]

4.122 While efforts are being made to educate staff in many agencies about the elements of the Code of Conduct and their duties in relation to disclosure of official information, there is room for improvement. Such training should not be limited to employees' duties in relation to disclosure of official information but should extend to cover all elements of the protective security standards.

The Commission's views

4.123 It would not be appropriate simply to direct APS employees to comply with the PSM as currently drafted, given the mix of general policy information, guidelines and recommendations that are not intended to be binding in nature, as well as purportedly mandatory standards. The ALRC proposes that, as a preliminary step, those standards intended to be mandatory should be clearly identified and modified as necessary. Once this process is complete, Agency Heads should direct all staff to comply with the mandatory standards. To reinforce that direction, agencies should ensure that the standards

---

135 Ibid, 21–22.
136 Ibid, 28–29.

are well understood and that both new and current employees receive regular training in complying with the standards.

4.124 In addition, given the potentially serious consequences for APS employees found to be in breach of mandatory protective security standards, the ALRC has formed the view that it would be appropriate to amend the APS Code of Conduct to add a new element stating that APS employees are required to comply with relevant protective security standards.

Proposal 4–11 The Attorney-General's Department should clearly identify, and modify as necessary, those protective security standards in the revised Commonwealth Protective Security Manual intended to be mandatory and enforceable. These standards should then be published in a manner that clearly indicates their mandatory and enforceable nature.

Proposal 4–12 Following the action described in Proposal 4–11, Agency Heads, or other officers with appropriate authority, should direct all staff to comply with those mandatory standards.

Proposal 4–13 To reinforce that direction, agencies should ensure that the standards are well understood and that both new and current employees receive regular training in complying with the standards.

Proposal 4–14 The Australian Government should amend the Australian Public Service Code of Conduct to add a new element stating that Australian Public Service employees are required to comply with the protective security standards described in Proposal 4–11.

Breach of contract

4.125 The APS Code of Conduct binds APS employees, Agency Heads and statutory office holders. It does not extend to those who perform functions or provide services under contract for the Government. While the minimum standards in the PSM might be enforced against APS employees through the Code of Conduct, this is not possible in relation to contractors and their employees.

4.126 Further, certain Australian Government agencies are not covered by the *Public Service Act*. Staff of ASIO, for example, are employed under the *Australian Security Intelligence Organisation Act 1979* (Cth) on the basis of written contracts with the Director-General of Security. Staff of ASIS are employed under the *Intelligence Services Act 2001* (Cth) on the basis of written contracts with the Director-General of ASIS. While the discussion below and the extracts from the PSM quoted below are aimed at contractors performing functions that have been outsourced on a competitive

basis, the principles may also be applied to employees working directly under contract with the Australian Government.

4.127 Part F of the PSM deals specifically with the security framework for competitive tendering and contracting (CTC). The PSM makes clear that:

> It is an agency responsibility to ensure that the protective security requirements of outsourced functions are explicit and that the contractor has the capacity to comply with these requirements. Appropriate security procedures, based on the nature of the function and the classification of the information, need to be negotiated with the contractor and settled **before** finalising the contract.[137]

4.128 The PSM also states that a contract between an agency and a contractor must clearly provide that the contractor is required to comply with the minimum standards for protecting security classified information as set out in the PSM. The standards are set out in a table at the end of Part F for ease of reference.[138] Any additional agency-specific security requirements are to be separately specified in the contract or in a schedule to the contract.[139] The PSM also states that:

> Underpinning every CTC agreement is a legal contract that sets out the 'rules' governing the relationship between the parties. Care is needed to ensure that the contract clearly defines the rights and obligations of each party and that it represents an agreed outcome for the agency and the contractor. The contract must include provisions on the confidentiality and security of official information and other resources ...[140]
>
> Agencies are ... 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][141]

4.129 The PSM includes some model contractual clauses but stresses that agencies should be aware of the limitations of example clauses and that it is not possible to draft standard documentation to suit all circumstances. In relation to security standards, the PSM suggests the following:

> 1. The Contractor agrees to comply with the security requirements for the protection of official information:
>
>   (a) detailed in the Protective Security Manual as minimum standards;
>
>   (b) set out in the Contract and in Schedule [ ]; and
>
>   (c) as advised by the Agency during the term of the Contract.

137 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), F 6, [1.6].
138 Ibid, F 57–60.
139 Ibid, F 37, [6.8].
140 Ibid, F 36, [6.1].
141 Ibid, F 36, [6.4].

> 2. The Contractor agrees to perform its security obligations under the Contract to the highest professional standards described or indicated in the requirements of the Protective Security Manual as amended from time to time.
>
> 3. The rights and obligations arising in connection with this clause [ ] will survive any termination or expiration of the Contract.
>
> 4. If the security requirements are redefined, the Contractor is entitled to apply to the Agency for a price variation.[142]

4.130 The PSM also provides for Employee Undertakings:

> Even if an agency feels confident that there are no security issues to be addressed in the contract, it should consider requiring specified contractor employees, particularly those requiring access to security classified information, to sign an Employee Undertaking or Deed of Confidentiality ... It is imperative that contractors and their employees and any subcontractors understand that any information used or generated under the contract belongs to the Commonwealth and must never be used for any purpose other than that determined by the Commonwealth agency with whom they have contracted.[143]

4.131 As discussed above, this mechanism could also be used to enforce the minimum standards against APS employees.

4.132 The PSM notes that, where compliance with the minimum standards in the PSM is part of a contractual agreement:

> Agencies should ensure that a clause is included in the contract clearly stating the obligations of both parties if the contractor fails to meet the security requirements.[144]
>
> Where there has been a security breach or violation on the part of the contractor or its employees, there are a number of measures available to the agency to minimise its consequences and prevent further security incidents. These could range from negotiation with the company's senior management about amending monitoring and disciplinary processes to moving the contract if the contractor is unable or unwilling to adapt internal processes and procedures to meet the agency's security requirements.[145]
>
> The agency must have a right to impose additional requirements on the contractor, or the entitlement to terminate the contract, if there is a failure to comply with security requirements specified in the contract.[146]

4.133 A contractor in serious or repeated breach of the PSM's security standards may find that its contract with the Australian Government is terminated or not renewed. The Government may be able to bring a civil suit for damages—although, in relation to a serious security breach, the amount would be difficult to assess and, in any event,

---

142 Ibid, F 38, [6.8].
143 Ibid, F 18, [4.14].
144 Ibid, F 31, [5.42].
145 Ibid, F 32, [5.43].
146 Ibid, F 50, [6.26].

unlikely to provide real compensation or penalty for the damage caused by the disclosure. It is also possible that an unauthorised disclosure could amount to a criminal offence in some circumstances.[147]

4.134 When dealing with classified or security sensitive information, the emphasis should be on preventive procedural safeguards rather than the imposition of penalties for breach. This is the approach adopted in the PSM, which recommends that agencies ensure that contractors are trained in security procedures and that agencies actively monitor contractors' performance on a regular basis. This includes requiring contractors to notify agencies of security breaches so that agencies can amend procedures or take other corrective action where necessary.

4.135 The ALRC has not received any information expressly indicating the inadequacy of the guidelines provided in the PSM in relation to contractors who are required to handle classified and security sensitive information. The *State of the Service Report 2001–02* noted more generally:

> In response to the Humphry Review, considerable attention has been focused on agencies' ability to maintain sufficient control over outsourced arrangements to enable them to meet their accountability responsibilities under the *Public Service Act 1999* and the FMA [Financial Management and Accountability] Act. This includes issues such as managing contractors according to the requirements of the APS Values and Code of Conduct, the ethical management of outsourcing and conflict of interest, managing intellectual property issues, attention to privacy concerns, risk management and audit activity.[148]

4.136 The Report does not specifically address the handling of classified and security sensitive information. However, in relation to the handling of personal information by contractors, it noted the following findings of the Office of the Federal Privacy Commissioner:

> The [Federal Privacy Commissioner's] audits assessed the physical and logical security controls of contracted service providers as inadequate. Some agencies did not have contractual arrangements in place with outsourced providers whose functions involved the handling of personal information on behalf of those agencies. The audits also commonly found that employees of contracted service providers and their subcontractors do not enter into deeds of confidentiality as required by Commonwealth contract. Finally the audit observed that personal information collected and stored by a contracted service provider on behalf of agencies is not returned to the agencies at the end of the contractual period.[149]

4.137 The Joint Committee of Public Accounts and Audit's inquiry into the management and integrity of electronic information in the Commonwealth is considering a number of serious breaches of information security including an alleged breach by a contractor, Telstra Enterprise Services Pty Ltd (TES), involving the loss of computer

147 See Ch 5.
148 Australian Public Service Commission, *State of the Service Report 2001–2002* (2002), 129.
149 Ibid, 133.

backup tapes in March 2003. Issues before the Committee included whether the contractual arrangements with TES were appropriate and the extent to which they were enforced.[150]

4.138 If the guidelines in the PSM are applied by agencies in their dealings with contractors, the minimum standards for the handling of classified and security sensitive information will form part of the legally binding relationship between the agency and the contractor. In these circumstances, the standards will be legally enforceable and the agency will have put in place appropriate mechanisms to monitor, amend and enforce the standards. The real question appears to be the extent to which agencies are complying with those guidelines in practice. The PSCC protective security survey contained a number of questions about agency mechanisms for ensuring contractors' compliance with the minimum standards—but, as noted above, the results of that survey are not publicly available.

The Commission's views

4.139 In line with Proposal 4–7 to Proposal 4–10 above, the ALRC's current view is that compliance with Australian Government protective security standards could be more effectively monitored through the APS Commission Agency Questionnaire and State of the Service reporting mechanism. The APS Commission should require agencies to report on compliance with the guidelines provided in Part F of the PSM in relation to contractors who have access to classified and security sensitive information. The questions should be developed in consultation with the PSCC and, possibly, ANAO, and could be based closely on questions in the existing PSCC protective security survey.

4.140 To the extent appropriate, the results of the Agency Questionnaire should be made public in the annual State of the Service Report. More detailed agency-specific information could be passed to PSCC for consideration with a view to providing agencies with specific advice on improving protective security performance by contractors.

4.141 The Inspector-General of Intelligence and Security would also need to be involved in relation to the intelligence agencies not subject to the jurisdiction of the APS Commissioner.

4.142 Agencies should be encouraged to schedule internal security auditing procedures in relation to contractors with these processes so that information collected as part of the internal audit can also be used to respond to the Agency Questionnaire.

---

150 *Transcript of Inquiry into Management and Integrity of Electronic Information in the Commonwealth by Joint Committee of Public Accounts and Audit*, 17 October 2003, 18 (Sen K Lundy).

Proposal 4–15 The Australian Public Service Commission Agency Questionnaire should be expanded to include a section on agency compliance with the guidelines provided in Part F of the revised Commonwealth Protective Security Manual in relation to contractors who have access to classified and security sensitive information. To the extent appropriate, the results of this section of the Questionnaire should be included in the annual State of the Service Report to the Prime Minister.

Proposal 4–16 The Inspector-General of Intelligence and Security should seek information from the intelligence agencies not subject to the jurisdiction of the Australian Public Service Commissioner on agency compliance with the guidelines provided in Part F of the revised Commonwealth Protective Security Manual in relation to contractors who have access to classified and security sensitive information. The results should be included in an annual report to the Prime Minister.

Proposal 4–17 The Protective Security Coordination Centre should scrutinise agency responses to the questionnaires and enquiries referred to in Proposals 4–15 and 4–16 with a view to providing agencies with advice on improving protective security performance by contractors.

Proposal 4–18 Agencies should be encouraged to schedule internal security auditing procedures in relation to contractors so that information collected as part of the internal audit can be used to respond to the annual Australian Public Service Commission and Inspector-General of Intelligence and Security Agency Questionnaires.

5. Prevention and Punishment of Unauthorised Disclosure

Contents

5.1 The previous chapter considered the protection of classified and security sensitive information in the administrative context and, in particular, the impact and effectiveness of the protective security standards in the *Commonwealth Protective Security Manual* (PSM). It also considered administrative and contractual mechanisms for enforcing those standards in the everyday course of business, including the imposition of administrative or contractual penalties for breach of the standards. This chapter examines the legislative provisions and other legal mechanisms available to prevent or punish unauthorised disclosures of official information and the extent to which those mechanisms may assist in protecting classified and security sensitive information.

5.2 These mechanisms are not part of the everyday administration of government business. They are extraordinary measures, usually involving the courts, and should be seen as measures of last resort. The need for them arises when administrative or contractual arrangements for the protection of classified and security sensitive information have broken down and unauthorised disclosure has occurred or is about to occur. While there is a place in a comprehensive risk management strategy for the use of the courts and tribunals to attempt to prevent disclosure in appropriate circumstances and for the use of the criminal law to impose penalties for unauthorised disclosure, priority must be given to ensuring that appropriate and effective administrative and contractual practices and procedures are in place. Preventing disclosure is far more valuable than imposing a penalty once the information has been disclosed. Furthermore, resorting to court action means that the classified and security sensitive information in question becomes subject to the disclosure requirements associated with those processes.

Prevention

5.3 This section will examine the civil law mechanisms available to the Australian Government to prevent unauthorised disclosure of classified or security sensitive information where, for example, the media are proposing to publish information which has been leaked.

5.4 One of the limits on the utility of the preventive mechanisms discussed below is that, in order to prevent disclosure by taking civil action in the courts, the Government must be aware that the disclosure is about to occur. In practice, this is not typically the case. Furthermore, the Government requires admissible evidence to support any court application it might make—which can be difficult to obtain.

5.5 In a 1994 Legal Practice Briefing,[1] the Australian Government Solicitor considered the various civil law mechanisms available to government to protect confidential information. These included an action in copyright and an action to recover property owned by the Government. The Briefing acknowledges that, in most cases, these mechanisms are unlikely to effectively address the potential damage caused by the unauthorised disclosure of confidential information. An action in copyright might be effective to restrain publication of government documents themselves,[2] but the information contained in them can be published without infringing the law of copyright so long as the publication does not reproduce the actual work[3] since copyright law protects the form of the work rather than the information.

5.6 The Legal Practice Briefing also notes that, while the Government could take action to recover a document or computer disk that was government property, this would not prevent the defendant from disclosing the contents of the document or from making his or her own copy of the document or disk.

5.7 The Briefing also examined two other possible mechanisms: an action for breach of confidence and an action for an injunction to restrain a breach of the criminal law. The utility of these mechanisms in protecting classified and security sensitive information is considered below.

Breach of confidence

5.8 In the High Court case *Commonwealth v Fairfax*, Mason J cited with approval the following formulation of the equitable principle of breach of confidence:

---

1 Australian Government Solicitor, *Legal Practice Briefing Number 14: Unauthorised Disclosure of Government Information* (1994) Commonwealth of Australia.

2 An interim injunction to restrain the publication of certain government documents was granted by the High Court in *Commonwealth v Fairfax* (1980) 147 CLR 39 on the grounds that publication would be a breach of copyright.

3 This in fact occurred in relation to the information subject to consideration in *Fairfax* when Richard Walsh and George Munster published much of the content of the documents in summary form in R Walsh and G Munster, *State Secrets: A Detailed Assessment of the Book They Banned, Documents on Australian Defence and Foreign Policy 1968–1975* (1982).

> The principle is that the court will 'restrain the publication of confidential information improperly or surreptitiously obtained or of information imparted in confidence which ought not to be divulged' (Lord Ashburton v. Pape (1913) 2 Ch 469, at p 475, per Swinfen Eady LJ).[4]

5.9 Unlike an action in copyright, an action for breach of confidence may be taken in relation to information itself, whether written or verbal. An action can also be brought against a third party to whom information has been communicated in breach of a duty of confidence where that third party was aware, or should reasonably have been aware, that the information was confidential. This allows action to be taken against publishing houses and media organisations, and many of the cases involving confidential government information have arisen in this context. There is a wide range of remedies available in breach of confidence actions including damages or an account of profits, an order for delivery-up or destruction of documents, and injunctions restraining publication. The discussion below focuses on injunctions restraining publication as the most useful mechanism for protecting classified and security sensitive information, but other orders may also be appropriate in particular cases.

5.10 The court's power to grant an injunction to prevent the disclosure of confidential government information was considered by Mason J in *Fairfax*.[5] In that case, *The Age* and *The Sydney Morning Herald* newspapers were proposing to publish extracts from an upcoming book, *Documents on Australian Defence and Foreign Policy 1968–1975*, including extracts from classified government documents dealing with the ANZUS Treaty and the East Timor crisis. Copies of the early editions of the newspapers had been distributed before the publishers received notice of the interim injunction restraining publication. The Australian Government had not authorised publication of the documents in question and sought injunctions to prevent further publication. The Government argued that the widespread disclosure of this information would prejudice Australia's relations with other countries, especially Indonesia and the United States. Mason J concluded that the information had probably been leaked by a public servant in breach of his or her duty and contrary to the security classifications marked on some of the documents.

5.11 The equitable action for breach of confidence was developed 'to protect the personal, private and proprietary interests of the citizen, not to protect the very different interests of the executive government'.[6] Mason J accepted that in some circumstances the principles could be applied to protect information in the hands of government, but stated that:

> the plaintiff must show, not only that the information is confidential in quality and that it was imparted so as to import an obligation of confidence, but also that there will be 'an unauthorised use of that information to the detriment of the party communicating it' (Coco v AN Clark (Engineers) Ltd (1969) RPC 41, at p 47). The question

4 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50.
5 Ibid.
6 Ibid, 51.

> then, when the executive government seeks the protection given by equity, is: What detriment does it need to show?[7]

5.12 Mason J held that disclosure of confidential information would be restrained at the instance of the Government if it appeared that disclosure would be 'inimical to the public interest because national security, relations with foreign countries or the ordinary course of business of government will be prejudiced'. However, he noted that:

> it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticize government action.
>
> Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.[8]

5.13 Mason J cited with approval the formulation of the principles by Lord Widgery CJ in *Attorney-General v Jonathan Cape Ltd*:

> The Attorney-General must show (a) that such publication would be a breach of confidence; (b) that the public interest requires that the publication be restrained, and (c) that there are no other facts of the public interest contradictory of and more compelling than that relied upon. Moreover, the court, when asked to restrain such a publication, must closely examine the extent to which relief is necessary to ensure that restrictions are not imposed beyond the strict requirement of public need.[9]

5.14 Mason J noted that this approach had been criticised on the ground that it unduly restricted the right of government to restrain disclosure of confidential information.[10] It has been suggested that the second and third elements of Lord Widgery's formulation 'may constitute substantial hurdles for a plaintiff to negotiate' and appear to place the burden of proof on the plaintiff to demonstrate the public interest in enforcing the obligation of confidence.[11] In any event, Mason J went on to consider whether publication of the documents would be contrary to the public interest. As noted in Chapter 4,[12] he did not place great weight on the fact that certain documents were classified, being of the view that, because security classifications were not regularly reviewed, many documents remained over-classified. In this case, he was not persuaded:

> that the degree of embarrassment to Australia's foreign relations which will flow from disclosure is enough to justify interim protection of confidential information.[13]

---

7 Ibid, 51.
8 Ibid, 52.
9 *Attorney-General v Jonathan Cape Ltd* [1976] QB 752, 770,771.
10 See M Bryan, 'The Crossman Diaries—Developments in the Law of Breach of Confidence' (1976) 92 *The Law Quarterly Review* 180.
11 Ibid, 181.
12 See Ch 4 at [4.55] above.
13 *Commonwealth v Fairfax* (1980) 147 CLR 39, 54.

5.15 Furthermore, the previous limited publication of the material meant that the detriment the plaintiff feared would not have been avoided by an injunction. This case has been described as illustrating 'the judicial reticence in restraining the disclosure of governmental information to the public'.[14]

5.16 In *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd*,[15] the Attorney-General for the United Kingdom sought an injunction to restrain publication in Australia of the book, *Spycatcher,* by Peter Wright, a former member of MI5 (the British Security Service). The majority of the NSW Court of Appeal dismissed the Attorney-General's appeal from an order refusing to grant an injunction to restrain publication of the book on a range of grounds including that much of the information had passed into the public domain. Interestingly, Street CJ, in his dissenting judgment, expressed the view that the case did not rest on establishing a breach of an equitable duty of confidence:

> The public right of the United Kingdom or Australian Government ... to protect its confidential information is not based on doctrines of contract or of equity. It is a right of a different character, deriving from the entitlement of a state and its organs to protection against harm to the public interest if such information be disclosed.
>
> The nature of the public right to protection is the same, whether it be advanced as a basis of a grant of substantive relief against disclosure, or whether it be advanced as a basis for resisting compulsory production of information in litigation between other parties.[16]

5.17 Kirby P, however, was prepared to consider the action for breach of confidence and cited with approval Mason J's formulation in *Fairfax*. He also cited with approval the dissenting judgment of Lord Denning in *Schering Chemicals Ltd v Falkman Ltd*:

> Freedom of the press is of fundamental importance in our society. It covers not only the right of the press to impart information of general interest or concern, but also the right of the public to receive it. It is not to be restricted on the ground of breach of confidence unless there is a 'pressing social need' for such restraint. In order to warrant a restraint, there must be a social need for protecting the confidence sufficiently pressing to outweigh the public interest in freedom of the press.[17]

5.18 Kirby P expressed the view that, given the nature of the information in this case, it was virtually impossible for the UK Government to overcome the defence of publication in the public interest:

> Looking at the issue through the eyes of Lord Denning, can there be any doubt that the public interest of Australia (whatever may be the public interest in the United Kingdom) requires or at least justifies the disclosure of the matters in Spycatcher? …

---

14 G Dal Pont and D Chalmers, *Equity and Trusts in Australia and New Zealand* (1996).

15 *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86.

16 Ibid, 92.

17 *Schering Chemicals Ltd v Falkman Ltd* [1982] QB 1, 22.

> The very intensiveness of the scrutiny to which ASIO and ASIS have been subjected in this country show that we, more perhaps than the United Kingdom, have asserted in recent years—under governments of differing political persuasion—an insistence upon the lawfulness of the operations of the security services, their accountability to the government and the parliament and their loyalty to the democratic nature of the country, whose mission it is theirs to defend. In these circumstances, it would be hard to conceive of matters of greater public interest and gravity than those revealed in *Spycatcher*.[18]

5.19 In the related UK case of *Attorney-General v Guardian Newspapers Ltd and others*,[19] the House of Lords refused to grant an injunction on the basis that the information had ceased to be confidential due to the publication of the book in Australia, the United States and elsewhere. The House of Lords adopted the approach of Mason J in *Fairfax* and made it clear that, in order to bring a successful action for breach of confidence, the Government would have to establish that disclosure would be contrary to the public interest. The House of Lords stated that, had the information still been confidential, the public interest in this case would not have justified disclosure.

5.20 One commentator has noted in relation to the *Spycatcher* cases that:

> The consequences of allowing the courts to weigh up the competing public interests in relation to the protection or disclosure of confidential information without the guidance of clear principles is exemplified in the *Spycatcher* decision ... the decision reached by the House of Lords regarding the public interest is in direct contrast to the judgement of Kirby P in the Australian litigation in which his Honour found that much of the information may have been disclosed on the basis of the public interest defence.[20]

5.21 While the Australian courts have been prepared in theory to extend the protection of breach of confidence to government information, they have made it clear that the interests to be balanced in relation to such information are different from those in cases involving private or commercial information. The Government as plaintiff in a breach of confidence action faces a much more difficult task in establishing its case given the public interests articulated by the courts in freedom of the press and public access to government information. An additional onus is imposed on the Government as plaintiff to establish that the balance of public interests favours protecting the information. Professor Dennis Pearce has pointed out that this approach differs from the courts' approach to confidential government information used as evidence and has commented in this regard:

> Why a different onus should exist in circumstances where, on the one hand, the Crown is resisting the admission in evidence of information and, on the other, is endeavouring to prevent the publication of information is not readily apparent unless it be the ordinary rule that it falls on the plaintiff to establish his case. If this is indeed

---

18 *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86, 170.

19 *Attorney-General v Guardian Newspapers Ltd and Others* [1988] 3 All ER 545.

20 K Koomen, 'Breach of Confidence and the Public Interest Defence: Is It In the Public Interest?' (1994) 10 *Queensland University of Technology Law Journal* 56, 67.

> the situation, it seems inappropriate when the basic question remains constant, namely, whether it is in the public interest that the particular information be revealed.[21]

Commission's views

5.22 The Australian and UK Governments have had little success in pursuing actions for breach of confidence in relation to unauthorised disclosures of confidential government information, even where the information is security classified. While the courts have articulated a set of principles that might protect confidential government information in some circumstances, in practice those circumstances appear to be fairly limited. This is because:

> although in the case of private citizens there is a public interest that confidential information should as such be protected, in the case of Government secrets the mere fact of confidentiality does not alone support such a conclusion, because in a free society there is a continuing public interest that the workings of the Government should be open to scrutiny and criticism. From this it follows that, in such cases, there must be demonstrated that some other public interest requires that publication should be restrained.[22]

5.23 While it might be argued that there is a public interest in allowing governments to protect confidential information except where a public interest defence can be established by the disclosing party, the courts have not adopted this approach. It is likely that the additional onus placed on a government as plaintiff in actions for breach of confidence acts as a disincentive to pursue such actions, and may explain the limited number of occasions on which the Australian Government has sought relief of this kind from the courts.

5.24 The ALRC has not included any proposals in relation to actions for breach of confidence in this Discussion Paper on the basis that there is an alternative and possibly more effective civil law mechanism available to prevent disclosure of classified and security sensitive information—that is, an injunction restraining a breach of the criminal law, discussed below. However, the ALRC would be interested in receiving further submissions on this issue.

Restraining breach of criminal law

5.25 The courts have traditionally been reticent about injunctions to restrain breaches of the criminal law:

> Equity has traditionally been reluctant to enjoin breaches of the criminal law. Lord Eldon's statement in *Gee v Pritchard* that 'equity will not enjoin a crime' represented and still represents an established principle of equitable discretion.[23]

---

21 D Pearce, 'The Courts and Government Information' (1976) 50 *Australian Law Journal* 513, 520.

22 *Attorney-General v Guardian Newspapers Ltd and Others* [1988] 3 All ER 545, 651.

23 J Duns, 'Enjoining Breaches of Criminal Legislation' (1990) 14 *Criminal Law Journal* 5, 5.

5.26 Lord Wilberforce justified this approach in *Gouriet v Union of Post Office Workers* as follows:

> If Parliament has imposed a sanction (for example, a fine of £1), without an increase in severity for repeated offences, it may seem wrong that the courts, civil courts, should think fit, by granting injunctions, breaches of which may attract unlimited sanctions, including imprisonment, to do what Parliament has not done. Moreover, where Parliament has (as here in the *Post Office Act* 1953) provided for trial of offences by indictment before a jury, it may seem wrong that the courts, applying a civil standard of proof, should in effect convict a subject without the prescribed trial.[24]

5.27 In *Commonwealth v Fairfax*, Mason J considered the issue of injunctions to restrain an actual or threatened breach of the criminal law. He stated that to grant such an injunction would be exceptional and generally confined to cases of emergency and those where the penalty was either inadequate or only supplemental to other relief. He also noted:

> It may be that in some circumstances a statutory provision which prohibits and penalizes the disclosure of confidential government information or official secrets will be enforceable by injunction. This is more likely to be the case when it appears that the statute, in addition to creating a criminal offence, is designed to provide a civil remedy to protect the government's right to confidential information. I do not think that s79 is such a provision. It appears in the Crimes Act and its provisions are appropriate to the creation of a criminal offence and to that alone. The penalties which it imposes are substantial. There is nothing to indicate that it was intended in any way to supplement the rights of the Commonwealth to relief by way of injunction to restrain disclosure of confidential information or infringement of copyright. There is no suggested inadequacy in these two remedies which would lead me to conclude that it is appropriate to regard s79 as a foundation for injunctive relief.[25]

5.28 Mason J was not prepared to issue an injunction on these grounds in this particular case. However, the courts have issued injunctions to restrain breaches of the criminal law—for example, where the breaches have continued despite the imposition of criminal penalties—on the basis that the penalty was inadequate to deter the continuing breaches.[26] In *John Fairfax Publication Pty Ltd v Doe*, the NSW Court of Appeal upheld the grant of an injunction restraining the publication of an intercepted telephone conversation on the basis that the publication would have a tendency to interfere with the conduct of pending criminal proceedings.[27] The conversation had been lawfully intercepted under the *Telecommunications (Interception) Act 1979* (Cth) but the newspaper publication of the conversation would have contravened s 63 of the Act, which placed strict limits on the use that could be made of such intercepted communications.

---

24 *Gouriet v Union of Post Office Workers* [1978] AC 435, 481.
25 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50.
26 *Attorney-General v Harris* [1961] 1 QB 74.
27 *John Fairfax Publication Pty Ltd v Doe* (1995) 37 NSWLR 81.

5.29 In its review of the use of civil and administrative penalties in federal regulation,[28] the ALRC identified 53 federal legislative provisions providing for injunctive relief. Some of these provisions allow courts to issue an injunction in relation to conduct which is also criminal; for example, s 383 of the *Commonwealth Electoral Act 1918* (Cth) and s 80 of the *Trade Practices Act 1974* (Cth). ALRC 95 notes that:

> Injunctions are not in themselves penalties but are used in support of actions seeking penalties. In consultations, ASIC officers have commented on the usefulness of injunctions in acting quickly against offenders.
>
> > 'The foundation of the ASIC approach is to try and protect investors, so the first step is always to act to protect, then start thinking about civil or criminal penalties.'
>
> The ACCC says that it is the public interest nature of a regulator's work that leads courts towards a willingness to grant injunctions.[29]

5.30 ALRC 95 also notes that in *ICI Australia Operations Pty Ltd v Trade Practices Commission*, the Federal Court concluded that the granting of an injunction under s 80 of the *Trade Practices Act* in addition to pecuniary penalties was appropriate:

> Injunctions are traditionally employed to restrain repetition of conduct. A statutory provision that enables an injunction to be granted to prevent the commission of conduct that has never been done before and is not likely to be done again is a statutory enlargement of traditional equitable principles. But this is because traditional doctrine surrounding the grant of injunctive relief was developed primarily for the protection of private proprietary rights. Public interest injunctions are different. Parts IV and V of the [Trade Practices] Act involve matters of high public policy. Parts IV and V relate to practices and conduct that legislatures throughout the world in different forms, and to different degrees, have decided are contrary to the public interest ... These are legislative enactments of matters vital to the presence of free competition and enterprise and a just society. This does not mean that the traditional equitable doctrines are irrelevant. For example, it must be relevant to consider questions of repetition of conduct or whether it has ever occurred before or whether imminent substantial damage is likely, but the absence of these elements is not fatal to the granting of an injunction under s 80.[30]

5.31 Many of these elements are also relevant to the protection of classified and security sensitive information. In considering whether to issue an injunction to protect such information, the court is not considering the protection of a private proprietary right but rather a matter of public interest. In considering the grant of such an injunction, it is relevant for the court to consider issues such as whether imminent substantial damage to, for example, national security is likely. In addition, the court would have to consider the adequacy of any criminal penalty imposed after the unauthorised disclosure

---

28 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, ALRC 95 (2002).

29 Ibid, 89.

30 *ICI Australia Operations Pty Ltd v Trade Practices Commission* (1992) ATPR 41–185, 40,524–40,525.

takes place on the basis that, once classified or security sensitive information has been disclosed, the damage is done and cannot be reversed.

Commission's views

5.32 In *Fairfax*, Mason J leaves open the possibility that the Government might revisit legislation dealing with unauthorised disclosure to provide expressly for the issue of injunctions to restrain such disclosure. Certain other Commonwealth legislation already provides for injunctions to restrain behaviour that is also criminal. Subject to the discussion below about the particular criminal provisions dealing with unauthorised disclosure of government information, the ALRC's preliminary view is that, where disclosure of classified and security sensitive information would amount to a criminal offence, it would be appropriate for the courts to be granted the express power to issue injunctions to restrain such disclosure before it occurs.

5.33 The need for injunctive relief is most likely to arise in relation to s 79 of the *Crimes Act*, discussed in detail below,[31] which deals with the unauthorised communication of official secrets by any person, including publishers and the media. It is less likely to arise in relation to other provisions dealing with unauthorised disclosure, for example, s 70 of the *Crimes Act* (which deals with unauthorised disclosure by Commonwealth officers) and s 91.1 of the *Criminal Code Act* (which deals with espionage), because, as a matter of fact, the Australian Government is less likely to become aware in advance that the disclosure is to take place. The proposal below is framed to include these provisions and to allow action to be taken in advance if, for example, the Government does become aware that unauthorised disclosure is likely to occur or where such disclosures are repeated on more than one occasion.

Proposal 5–1 Sections 70 and 79 of the *Crimes Act 1914* (Cth) and s 91.1 of the *Criminal Code Act 1995* (Cth) should be amended to provide that, where the courts are satisfied that a person has disclosed or is proposing to disclose classified or security sensitive information in contravention of the criminal law, the courts may grant an injunction to restrain such disclosure or further disclosure.

Deterrence and punishment

5.34 The Terms of Reference ask the ALRC to examine the operation of existing mechanisms designed to prevent the unnecessary disclosure of classified or security sensitive information in the course of criminal investigations and court proceedings. An essential element of this part of the Inquiry is to examine the relevant criminal provisions themselves to ensure that they are appropriate and workable and provide the

31 See [5.71] below.

correct balance in relation to the need to disclose classified and security sensitive information in the course of an investigation or prosecution.

5.35 As noted in Chapter 4,[32] a breach of the protective security standards in the *Commonwealth Protective Security Manual* (PSM)[33] may also amount to a breach of the criminal law relating to the handling of official information in some circumstances.

5.36 Criminal offences may be structured in one of three ways:

- *Mens rea* offences: where the prosecution must prove fault elements (the mental element) as well as the physical element (*actus reus*);

- Strict liability offences: where the prosecution is not required to prove any fault elements but where a defence of reasonable mistake, and possibly other statutory defences such as due diligence, are available; and

- Absolute liability offences: where proof of fault is not required and the defence of reasonable mistake is not available.

5.37 A further distinction is drawn between summary and indictable offences. Summary offences are those of a less serious nature—they are tried before a magistrate sitting without a jury, and attract lower penalties. The vast majority of criminal matters are summary. Indictable offences are more serious, attract higher penalties and, in general, must be tried before a judge and jury. Section 80 of the *Australian Constitution* states that:

> The trial on indictment of any offence against any law of the Commonwealth shall be by jury, and every such trial shall be held in the State where the offence was committed, and if the offence was not committed within any State the trial shall be held at such place or places as the Parliament prescribes.[34]

5.38 The *Crimes Act 1914* (Cth) defines indictable offences as those punishable by imprisonment for a period of more than 12 months unless the contrary intention appears.[35] Summary offences are defined as those not punishable by imprisonment or punishable by imprisonment for less than 12 months, unless the contrary intention appears.[36] Certain indictable offences may be dealt with summarily, for example, with the consent of the prosecutor and the defendant, although this is not possible in relation to s 79(2) or 79(5), discussed further below.[37]

---

32 See [4.98] above.
33 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000).
34 Section 80 of the *Australian Constitution* is discussed further in Ch 7.
35 *Crimes Act 1914* (Cth), s 4G.
36 Ibid, s 4H.
37 Ibid, s 4J(7).

5.39 The *Criminal Code Act 1995* (Cth) contains general principles of criminal responsibility under the laws of the Commonwealth. Commonwealth legislation creating an offence must be read alongside the *Criminal Code* to fully understand a person's legal rights and obligations.

5.40 Three provisions in the Commonwealth criminal law create general offences in relation to the unauthorised disclosure of official information:

- section 70 of the *Crimes Act*;
- section 79 of the *Crimes Act*; and
- section 91.1 of the *Criminal Code Act*.

5.41 There are also many other secrecy provisions in other Commonwealth legislation dealing with unauthorised disclosure in particular circumstances,[38] for example:

- section 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth), which binds ASIO officers, employees and contractors;
- section 39 of the *Intelligence Services Act 2001* (Cth), which binds employees, agents or contractors of the Australian Secret Intelligence Service (ASIS);
- section 40 of the *Intelligence Services Act*, which binds staff and contractors of the Defence Signals Directorate (DSD);
- section 34 of the *Inspector-General of Intelligence and Security Act 1986* (Cth), which binds the Inspector-General and staff; and
- section 58 of the *Defence Force Discipline Act 1982* (Cth), which binds members of the defence forces.[39]

5.42 These provisions have been reviewed on a number of occasions; for example, by the Gibbs Committee, which reported in 1991,[40] and the House of Representatives Standing Committee on Legal Constitutional Affairs, which reported in 1995.[41] The House of Representatives Standing Committee noted in its report that:

---

38 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs noted that there were over 150 specific secrecy provisions in Commonwealth statutes. House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth* (1995), 22.

39 These provisions are set out in Appendix 3.

40 Attorney-General's Department, *Review of Commonwealth Criminal Law: Final Report* (1991).

41 House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth* (1995).

> There was some comment to the effect that agencies would generally use the secrecy provisions in their own statutes to prosecute the unauthorised disclosure of confidential information and would only refer serious breaches to the AFP [Australian Federal Police] for prosecution under the general Crimes Act provisions.[42]

5.43 There have been very few prosecutions in Australia concerning the unauthorised disclosure of official information. This may be because, where the disclosure is by a Commonwealth officer, the matter is more often dealt with administratively. In 1998, Senator Robert Ray asked a series of questions on notice in the Senate seeking information on the number of times various departments had referred unauthorised disclosures of official information to the Australian Federal Police (AFP) for investigation between March 1996 and October 1998. Senator Ray also asked how many officers were charged with offences relating to unauthorised disclosures in this period. Although 56 matters were referred to the AFP for investigation by the 16 agencies that responded, only three resulted in charges being laid, all of which involved officers from the Department of Immigration and Multicultural Affairs.[43]

Unauthorised disclosure by Commonwealth officers

5.44 Section 70 of the *Crimes Act* is a general prohibition against unauthorised disclosure of official information by current and former Commonwealth officers. It provides that:

> (1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he is authorized to publish or communicate it, any fact or document which comes to his knowledge, or into his possession, by virtue of being a Commonwealth officer, and which it is his duty not to disclose, shall be guilty of an offence.
>
> (2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him), any fact or document which came to his knowledge, or into his possession, by virtue of having been a Commonwealth officer, and which, at the time when he ceased to be a Commonwealth officer, it was his duty not to disclose, shall be guilty of an offence.
>
> Penalty: Imprisonment for 2 years.

5.45 A Commonwealth officer for the purposes of s 70 is defined broadly as 'a person holding office under, or employed by, the Commonwealth' and includes a person performing services for or on behalf of the Commonwealth, such as a contractor, the officers and employees of ASIO[44] and staff of ASIS.[45] Behaviour that contravenes s 70 of the *Crimes Act* is also likely to be in breach of the APS Code of Conduct and may

---

42 Ibid.

43 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), Appendix 2.

44 *Australian Security Intelligence Organisation Act 1979* (Cth), s 91.

45 *Intelligence Services Act 2001* (Cth), s 38.

also contravene reg 2.1 of the *Public Service Regulations*.[46] While a breach of the *Public Service Act* or *Regulations* may attract a range of administrative penalties, a breach of s 70 is a criminal offence and may attract a penalty of up to two years' imprisonment.

5.46 Section 70 applies to information acquired by a Commonwealth officer in the course of the officer's duties and which the officer has a duty not to disclose. This may include, but is not limited to, classified and security sensitive information. Unlike some of the specific secrecy and espionage provisions discussed below, s 70 does not specifically limit the categories of official information included in the prohibition. For example, s 70 does not expressly distinguish between the disclosure of information that is likely to harm the public interest and information that is not. However, 'these are matters which may bear on whether a prosecution is instituted and on the penalty imposed by a court'.[47]

5.47 Section 70 has traditionally been given a broad interpretation:

> The traditional view has been that s 70 forbids disclosure, regardless of the nature of the information and the extent to which the public interest may be served by disclosure.[48]

5.48 In *Commissioner of Taxation v Swiss Aluminium Australia Ltd & Ors*, Bowen CJ in the Federal Court commented that:

> From the policy point of view it may be noted that an enactment such as s 70 of the *Crimes Act* prohibiting the disclosure of information obtained in the course of the duties of a public servant treats the nature or kind of information disclosed as virtually irrelevant. It is the office occupied by the person and the character in which he obtained the information which imposes the obligation of secrecy upon him in the interests of orderly administration and discipline of the service.[49]

5.49 By contrast, however, Higgins J in the ACT Supreme Court has expressed the view that certain limits are implied in s 70:

> Whether a duty of confidentiality arises so that s 70 *Crimes Act* can punish its breach will depend on the type of information, the circumstances in which it has been acquired and the interests of relevant parties in keeping it confidential. A consideration of the public interest must also be relevant. The duty to keep information confidential may attach to information of any kind but it must be such and acquired in such cir-

---

46 Note, however, that the validity of reg 2.1 has been thrown into serious doubt by the decision of the Federal Court in *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433. This issue is discussed further in Ch 4.

47 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49.

48 A Matthew, 'Closing the Gap between the Equitable Obligation of Confidence and the Crimes Act' (2001) 21 *Proctor* 12.

49 *Commissioner of Taxation v Swiss Aluminium Australia Ltd & Ors* (1986) 10 FCR 321.

> cumstances that such a duty arises. It does not arise merely because the information is obtained by an officer in the course of his or her duties.[50]

5.50 The situation is complicated by the fact that s 70 does not itself give rise to the duty not to disclose official information. This duty must be found elsewhere and may arise in a number of ways:

- the implied common law duty of fidelity and good faith owed by an employee to his or her employer;
- an express contractual duty;
- an equitable duty of confidence;[51] or
- specific legislative or regulatory provisions giving rise to a duty not to disclose official information.

5.51 The common law duty of fidelity and good faith is implied into all contracts of employment and includes a duty not to disclose or misuse confidential information. In *Bennett*, Finn J noted in relation to the common law duty of public sector employees:

> It probably is the case that such reasonable expectations that a government could entertain of its employees and which might give substance to the duty in a given case, are likely to be found in now commonplace codes of conduct and guidelines issued to employees (subject of course, to the accuracy, legality and reasonableness of the relevant code provisions).[52]

5.52 However, Finn J also stated that the common law duty would not arise in the context of confidential government information unless disclosure was likely to harm the public interest. This is more likely to be the case in relation to classified and security sensitive information although, as with the equitable duty of confidence, the issue would be one for the courts to decide in each particular case.

5.53 The equitable duty of confidence is discussed in detail in Chapter 4. The courts have also limited the equitable duty imposed on public sector employees to circumstances in which disclosure is likely to harm the public interest.

5.54 A duty not to disclose government information is also found in a range of legislative and regulatory provisions. The general duty is set out in reg 2.1 of the *Public Service Regulations*. However, the validity of this regulation is now in doubt following the decision in *Bennett*, in which reg 7(13)—which preceded reg 2.1 and is in almost identical terms—was held to be invalid.[53] Finn J struck down reg 7(13) on the basis

---

50 *Deacon v Australian Capital Territory* [2001] ACTSC [87].
51 Discussed in Ch 4
52 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433, [125].
53 Ibid.

that it was too wide and imposed an unnecessary and unreasonable burden on the implied constitutional right to freedom of communication about government and political matters. Until this matter is resolved, either on appeal or by amendment of the regulation, it would be unwise to rely on reg 2.1 as the basis of a duty for the purposes of s 70 of the *Crimes Act*.

5.55 A duty not to disclose may also be found in other specific secrecy provisions, including those set out above.[54] These provisions vary greatly in the way they are expressed. Some of them are expressed in fairly general terms, for example, s 18(2) of the *Australian Security Intelligence Organisation Act*, which provides:

> If a person makes a communication of any information or matter that has come to the knowledge or into the possession of the person by reason of his or her being, or having been, an officer or employee of the Organisation or his or her having entered into any contract, agreement or arrangement with the Organisation, being information or matter that was acquired or prepared by or on behalf of the Organisation in connection with its functions or relates to the performance by the Organisation of its functions, other than a communication made:
>
> (a) to the Director-General or an officer or employee of the Organisation:
>
> (i) by an officer or employee of the Organisation—in the course of the duties of the officer or employee; or
>
> (ii) by a person who has entered into any such contract, agreement or arrangement—in accordance with the contract, agreement or arrangement;
>
> (b) by a person acting within the limits of authority conferred on the person by the Director-General; or
>
> (c) with the approval of the Director-General or of an officer of the Organisation having the authority of the Director-General to give such an approval;
>
> the first-mentioned person is guilty of an offence.
>
> Penalty: Imprisonment for 2 years.

5.56 Sections 39 and 40 of the *Intelligence Services Act* in relation to ASIS and the DSD are in broadly similar terms. The categories of information covered by these provisions are very wide; that is, information connected with or relating to the performance of the organisations' functions. The provisions do not distinguish between the disclosure of information that is likely to harm the national interest and information that is more benign.

5.57 By way of contrast, s 58 of the *Defence Force Discipline Act* provides that:

> (1) A person who is a defence member or a defence civilian is guilty of an offence if:

54 See [5.41].

> (a) the person discloses information; and
>
> (b) there is no lawful authority for the disclosure; and
>
> (c) the disclosure is likely to be prejudicial to the security or defence of Australia.
>
> Maximum punishment: Imprisonment for 2 years.
>
> (2) Strict liability applies to paragraph (1)(c).
>
> Note: For *strict liability*, see section 6.1 of the *Criminal Code.*
>
> (3) It is a defence if the person proves that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to be prejudicial to the security or defence of Australia.
>
> Note: The defendant bears a legal burden in relation to the matter in subsection (3). See section 13.4 of the *Criminal Code*.

5.58 This provision limits the circumstances in which unauthorised disclosure of official information by members of the defence force or defence civilians will amount to a criminal offence. Disclosure will only amount to a criminal offence when it is likely to be prejudicial to the security or defence of Australia and the person knew, or could reasonably be expected to have known, that the disclosure was likely to be prejudicial to the public interest in this way.

5.59 Specific secrecy provisions such as these are discussed further below.[55] These examples are provided to illustrate the variety of provisions upon which the Australian Government might need to rely to support a legislative duty for the purposes of s 70 of the *Crimes Act*.

5.60 The House of Representatives Standing Committee on Legal and Constitutional Affairs has noted the longstanding need for reform of s 70:

> The need for reform of section 70 has been recognised for some time. In 1979 the Senate Standing Committee on Legal and Constitutional Affairs recommended that section 70 be amended to limit the categories of information that it is an offence to disclose ... In 1983 the Human Rights Commission recommended that section 70 be limited to restrictions which are necessary to protect the rights and reputations of others and to protect national security, public order or public health or morals.[56]

5.61 In a submission to that inquiry, the Commonwealth Director of Public Prosecutions noted that prosecutions under s 70 were:

---

55 See [5.96] and following.

56 House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth* (1995), 90, 91.

> very difficult to get off the ground ... magistrates and other judicial officers tend to regard it as being such a broad provision as to perhaps impact adversely on its utility.[57]

5.62 The Gibbs Committee report concluded that:

> It is undesirable that the sanctions and machinery of the criminal law should be applied in relation to the unauthorised disclosure of all forms of official information and this should be avoided if possible.[58]
>
> ... the application of criminal sanctions under the general criminal law of the Commonwealth to disclosure of official information should be limited to certain categories of information and that these should be no more widely stated than is strictly required for the effective functioning of Government.[59]

5.63 The Committee went on to consider what categories of information should be protected by criminal sanctions. These included information relating to intelligence and security services, defence or foreign relations, and information obtained in confidence from other governments or international organisations.

Commission's views

5.64 The ALRC agrees with the Gibbs Committee that it is undesirable that the sanctions and machinery of the criminal law should be applied to the unauthorised disclosure of all official information. These should be reserved for official information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest. This approach is consistent with Australian Government policy as stated in the PSM and discussed in detail in Chapter 4.

5.65 Section 70 of the *Crimes Act*, while expressed in general terms, is not unlimited in its scope in the same way as reg 7(13) of the *Public Service Regulations*, which was considered in *Bennett*.[60] Unauthorised disclosure of government information will amount to a criminal offence under s 70 only where the officer has a duty not to disclose the information. The statement by Higgins J in *Deacon v Australian Capital Territory*, quoted above,[61] indicates the possibility that the courts will impose implied limits on the duty set out in s 70, but this remains uncertain.

5.66 Consequently, the ALRC believes that it would be appropriate to clarify the scope of the duty not to disclose official information for the purposes of the criminal law. This could be achieved in a number of ways, including by expressly defining the scope of the duty in s 70 or by ensuring that, where the duty arises from a secondary source, that source includes appropriate limits. The ALRC's current view is that there should be a certain amount of flexibility in the scope of the duty imposed on officers of

---

57 Ibid, 90.
58 Attorney-General's Department, *Review of Commonwealth Criminal Law: Final Report* (1991), 315.
59 Ibid, 317.
60 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433.
61 See [5.49].

certain agencies; for example, it may be appropriate to impose a more extensive duty on officers employed by the intelligence and security agencies than on other public servants. For this reason, the Proposals below do not focus on amending s 70 although the ALRC would be interested in receiving further submissions on this point.

5.67 Where the duty not to disclose government information is based on an employee's common law duty of fidelity and good faith or on an equitable duty of confidentiality, the courts have already indicated that a balance must be found between the public interest in protecting confidential government information and the public interest in the freedom of the press and open government.

5.68 Duties based on legislative provisions vary widely in the way they are expressed and the obligations they impose. While some of these provisions are criminal, other key provisions such as reg 2.1 of the *Public Service Regulations* are not. Although a certain amount of flexibility in the scope of specific secrecy provisions may be sensible, the Federal Court has struck down 'catch all' provisions which do not appropriately balance the need to protect government information with the implied constitutional freedom to communicate on government and political matters.[62]

5.69 Following *Bennett*, it would seem timely for the Australian Government to undertake a comprehensive review of secrecy provisions in Commonwealth legislation and regulations, including in particular reg 2.1 of the *Public Service Regulations*, the validity of which has been called into serious question by that decision. In conducting this review, the Government should ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest in some way. That harm could be defined as harm to the security, defence and international relations of Australia. These limits reflect the minimum standards in the PSM and are more likely to be consistent with the constitutional requirements at issue in *Bennett*. This approach would also help to ensure that the sanctions and machinery of the criminal law are only applied in sufficiently serious circumstances.

5.70 A further issue is that the duty imposed by reg 2.1 may also give rise to administrative sanctions under the *Public Service Act*. A clear distinction should be drawn in the regulations between conduct giving rise to administrative sanctions and conduct leading to criminal sanctions.

62 *Bennett v President, Human Rights and Equal Opportunity Commission* [2003] FCA 1433.

Proposal 5–2 The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information, including in particular regulation 2.1 of the *Public Service Regulations*, to ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.

Proposal 5–3 In conducting the review recommended in Proposal 5–2, the Australian Government should ensure that a clear distinction is drawn between conduct that gives rise to administrative sanctions under the *Public Service Act 1999* (Cth) and conduct that gives rise to criminal sanctions, including those under section 70 of the *Crimes Act 1914* (Cth).

Unauthorised communication of official secrets

5.71 Section 79 of the *Crimes Act* prohibits unauthorised communication of official secrets by any person.[63] Section 79(1) defines certain material or information as an 'official secret' if:

> (a) it has been made or obtained in contravention of this Part or in contravention of section 91.1 of the *Criminal Code*;
>
> (b) it has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he has made or obtained it owing to his position as a person:
>
> (i) who is or has been a Commonwealth officer;
> (ii) who holds or has held office under the Queen;
> (iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;
> (iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or
> (v) acting with the permission of a Minister;
>
> and, by reason of its nature or the circumstances under which it was entrusted to him or it was made or obtained by him or for any other reason, it is his duty to treat it as secret; or
>
> (c) it relates to a prohibited place or anything in a prohibited place and:
>
> (i) he knows; or
> (ii) by reason of its nature or the circumstances under which it came into his possession or control or for any other reason, he ought to know;
>
> that it should not be communicated to a person not authorized to receive it.

63 Section 79 is set out in Appendix 3.

5.72 An official secret may include 'a sketch, plan, photograph, model, cipher, note, document or article' or information.

5.73 The definition of an 'official secret' in s 79(1) limits the circumstances in which an unauthorised communication of official information will amount to a criminal offence under s 79. For example, the information must have been made or obtained in contravention of Part VII of the *Crimes Act* (which includes s 79) or s 91.1 of the *Criminal Code*, or the nature of the information or the circumstances under which it was obtained must give rise to a duty to treat the information as secret.

5.74 Despite this, the Gibbs Committee noted in its final report that:

> No distinction is drawn for the purposes of these provisions between information the disclosure of which may cause real harm to the public interest and information the disclosure of which may cause no harm whatsoever to the public interest.[64]

5.75 A Commonwealth officer, or any other person in possession of official secrets (including media organisations), may be guilty of an offence under s 79.[65] Section 79 creates a number of offences that attract penalties ranging from six months' to a maximum of seven years' imprisonment including:

- retaining material containing official secrets where there is no right or duty to retain it, failing to comply with a lawful direction to destroy such material or failing to take reasonable care of such material—maximum penalty: six months' imprisonment;[66]

- communicating, or allowing someone to have access to, an official secret where there is no authority or duty to communicate it—maximum penalty: two years' imprisonment;[67]

- receiving an official secret knowing, or having reasonable grounds to believe, that it is communicated in contravention of s 79(3)—maximum penalty: two years' imprisonment;[68]

- communicating, or allowing someone to have access to, an official secret with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions, where there is no authority or duty to communicate it—maximum penalty: seven years' imprisonment;[69] and

---

64 Attorney-General's Department, *Review of Commonwealth Criminal Law: Final Report* (1991), 242.

65 In *Commonwealth v Fairfax* (1980) 147 CLR 39, discussed above, one of the issues considered by Mason J was whether to issue an injunction to restrain the newspaper publishers from potentially committing a breach of s 79.

66 *Crimes Act 1914* (Cth), s 79(4).

67 Ibid, s 79(3).

68 Ibid, s 79(6). It is a defence to prove that the communication was contrary to the recipient's desire.

69 Ibid, s 79(2).

- receiving an official secret knowing, or having reasonable grounds to believe, that it is communicated in contravention of s 79(2)—maximum penalty: seven years' imprisonment.[70]

5.76 The Gibbs Committee's final report noted that there have been few successful prosecutions under s 79. Simon Lappas was charged with, and pleaded guilty to, offences under s 79(3). He was also prosecuted for offences under s 78 of the *Crimes Act* (which was subsequently repealed and replaced, although not in identical terms, by s 91.1 of the *Criminal Code Act*).[71]

5.77 Sections 79(3) and 79(6) do not include a subjective element of intention to harm the public interest or any objective requirement that the unauthorised communication is likely to harm the public interest. However, the material or information must be an 'official secret' and this primarily relates to whether the information itself, or the circumstances under which it is communicated, give rise to a duty to treat the information as secret. This duty is not necessarily the same as the duty in s 70, although there may be some overlap in the case of Commonwealth officers or private contractors who have given parallel undertakings. In relation to people who are not Commonwealth officers, the source and nature of this duty is unclear.

5.78 In bringing a charge against a Commonwealth officer under s 79(3), it is sufficient to prove that the document or information was an 'official secret' and that the information was communicated where there was no authority or duty to communicate it. Because of this, the actual content of the document or information is less likely to be an issue at trial. This appears to have been a relevant factor in the *Lappas* case, although there is little on the public record in relation to his conviction under s 79(3) as he pleaded guilty to those charges.[72]

5.79 Not all material or information that falls within the existing definition of 'official secrets' would harm the public interest if disclosed. Information may have been obtained in contravention of s 79, for example, but may no longer be sensitive due to the passage of time, prior disclosure in Australia or overseas, or some other reason. Nevertheless, communicating this information remains an offence under s 79(3). The introduction of an objective element that disclosure of the official secret was likely to harm the public interest would make it more probable that the nature and content of the disclosure would itself become a contested issue at trial—with a concomitantly greater risk that the court would have to take steps to protect classified or security sensitive information.

5.80 Sections 79(2) and 79(5), which attract the highest maximum penalty under s 79 of seven years' imprisonment, include an element of intent—that is, an 'intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's

---

70 Ibid, s 79(5). It is a defence to prove that the communication was contrary to the recipient's desire.
71 *R v Lappas and Dowling* [2001] ACTSC 115, *R v Lappas* [2003] ACTCA 21.
72 See Appendix 4.

dominions.' These provisions do not, however, require the unauthorised communication to be objectively likely to harm the public interest. This is consistent with the approach adopted in s 91.1 of the *Criminal Code Act*, discussed below, and with general criminal law policy in relation to individual culpability and criminal intention.

5.81 The Criminal Code Amendment (Espionage and Related Offences) Bill 2001 was intended, among other things, to repeal and replace s 79. Following controversy over its terms, the provisions relating to the unauthorised communication of official secrets were removed.[73] In introducing the Criminal Code Amendment (Espionage and Related Offences) Bill 2002, the then Attorney-General, the Hon Daryl Williams AM QC MP, stated that:

> Unlike the [earlier] bill … this bill does not amend the official secrets provisions currently contained in section 79 of the Crimes Act.
>
> Recently concerns have been raised about the official secrets provisions in that bill. These provisions were intended to replicate the substance of the official secrets provisions currently contained in section 79 of the Crimes Act. There has been considerable media attention focused on the perceived impact that the official secrets provisions in the earlier bill were alleged to have on the freedom of speech and on the reporting of government activities.
>
> The original bill did not alter the substance of the official secrets offences; it simply modernised the language of the offences consistent with the Criminal Code. The government's legal advice confirms that there was in substance no difference between the current provisions of the Crimes Act and the proposed provisions of the Criminal Code. The allegations ignore the fact that the existing law has not prevented the reporting of such stories in the past. Despite this, to avoid delay in the reintroduction of the important espionage provisions, the government decided to excise the official secrets provisions from the bill so only those relating to espionage have been included in the bill introduced today.[74]

Commission's views

5.82 Section 79 contains a number of offences dealing with unauthorised communication of official secrets of varying degrees of seriousness (as evidenced by the attached penalties). While the ALRC supports the principles underlying this general framework, s 79 is clearly due for reconsideration and reform. The language and structure of s 79 is complex and in some instances archaic. The source of the duty in certain sections is unclear, particularly in relation to people who are not Commonwealth officers. The extent to which s 79 overlaps with s 70 of the *Crimes Act* and s 91.1 of the *Criminal Code Act* is also unclear.

---

73 Senate Legal and Constitutional Legislation Committee, *Consideration of Legislation Referred to the Committee: Provisions of the Criminal Code Amendment (Espionage and Related Offences) Bill 2002* (2002), 1.

74 Commonwealth, *Parliamentary Debates*, House of Representatives, 13 March 2002, 1111 (A-G The Hon Daryl Williams AM QC MP).

5.83 The Australian Government recognised the need for reform of this provision in introducing the Criminal Code Amendment (Espionage and Related Offences) Bills 2001 and 2002.

5.84 While s 70 deals with unauthorised disclosure of official information by Commonwealth officers, s 79 imposes criminal sanctions on any person or organisation, including the media. It is essential that a provision of this kind is clear on its face and draws an appropriate balance between the need to protect sensitive government information and other public interests such as appropriate public access to government information. This will be particularly important if, as is suggested in Proposal 5–1, the law is amended to allow courts to grant injunctions in order to prevent an anticipated breach.

5.85 The more serious offences under s 79, which attract a maximum penalty of seven years' imprisonment, require an intention to prejudice the security or defence of Australia. It would be very difficult for the Crown to establish such an intention in relation to public discussion and disclosure of government information by the media. It is more likely that the media would be prosecuted under s 79(2), (4) or (6). The ALRC's preliminary view is that it would be appropriate to limit these offences to circumstances in which disclosure of the information is likely to harm the public interest.

5.86 The Australian Government should initiate a comprehensive review of s 79 of the *Crimes Act* to ensure that an appropriate public policy balance is found. Such a review should consider, among other things:

- whether criminal liability should require a finding that the unauthorised communication was objectively likely to, or did in fact harm the security or defence of Australia; and

- the relationship of s 79 with s 70 of the *Crimes Act* and s 91.1 of the *Criminal Code Act*.

Proposal 5–4 The Australian Government should initiate a comprehensive review of s 79 of the *Crimes Act* to ensure that an appropriate public policy balance is found. Such a review should consider, among other things:

(a) whether criminal liability should require a finding that the unauthorised communication was objectively likely to, or did in fact harm the security or defence of Australia; and

(b) the relationship of s 79 with s 70 of the *Crimes Act* and s 91.1 of the *Criminal Code Act*.

Espionage

5.87 Section 91.1 of the *Criminal Code Act 1995* (Cth) contains the major offences relating to espionage. These offences were removed from the *Crimes Act* as part of the reforms included in the *Criminal Code Amendment (Espionage and Related Offences) Act 2002*.[75] The new *Criminal Code Act* updated the terminology and concepts contained in the previous *Crimes Act* provisions, including the replacement of references to 'plans, photographs, models, ciphers, notes, documents and articles' with the broader terms 'information' and 'records', and removal of archaic references to 'the Queen's dominions'.

5.88 Section 91.1 of the *Criminal Code Act* and s 79 of the *Crimes Act* now refer to communicating information about Australia's 'security or defence'. Previously, s 78 and 79 of the *Crimes Act* referred to '*safety* or defence'. 'Security or defence' of a country is defined to include:

> the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies.[76]

5.89 Significantly, the maximum penalties for espionage offences were also increased from seven to 25 years' imprisonment.

5.90 Section 91.1(1) makes it an offence for any person to communicate or make available information concerning the security or defence of Australia—or information concerning the security or defence of another country which the person acquired, directly or indirectly, from the Australian Government—to another country or foreign organisation with the intention of prejudicing the security or defence of Australia.

5.91 Section 91.1 also creates a number of other offences:

- communicating or making such information available, without lawful authority, intending to give an advantage to another country's security or defence;
- making, obtaining or copying a record of such information with the intention of delivering it to another country or foreign organisation in order to prejudice the security or defence of Australia; and
- making, obtaining or copying a record of such information with the intention of delivering it to another country or foreign organisation, without lawful authority, in order to give an advantage to another country's security or defence.

---

75 Espionage offences had previously been found in Part VII of the *Crimes Act 1914* (Cth). Notably, s 78 of the *Crimes Act 1914* (Cth) was repealed and re-enacted, albeit in somewhat different terms and with significantly higher penalties, as s 91.1 of the *Criminal Code*. Simon Lappas was charged under s 78 and 79 of the *Crimes Act 1914* (Cth) as his offences occurred before the reforms in 2002.

76 *Criminal Code Act 1995* (Cth), s 90.1(1).

5.92 Section 91.2 provides a defence to a prosecution under s 91.1 where the defendant can show that the information had already been made available to the public with the authority of the Australian Government.

5.93 The Criminal Code Amendment (Espionage and Related Offences) Bill 2002 was referred to the Senate Legal and Constitutional Legislation Committee for inquiry and report in March 2002. The Committee's report noted that:

> Submissions and evidence before the Committee raised a number of issues in relation to the Bill. These were primarily that the Bill, if enacted, should not circumscribe civil liberties, particularly liberty to dissent, express dissent, and draw attention to unacceptable conduct by defence and intelligence services, whether in Australia or overseas.[77]

5.94 The concerns raised included: the definition of 'security and defence'; the use of the word 'prejudice'; the need for a defence in relation to information disclosed in the public interest; and the possibility that the offences could theoretically apply to information already in the public domain. The Committee considered all of the issues raised and made a range of recommendations, a number of which are reflected in the amendments made to the Bill.

Commission's views

5.95 To date, the ALRC has not received any submissions specifically raising concerns with s 91.1 of the *Criminal Code Act*. The provision was the subject of public inquiry and report by the Senate Legal and Constitutional Affairs Legislation Committee during its passage through the Parliament in 2002. The issues raised before the Senate Committee were fully considered and the provisions as currently drafted appear to draw an appropriate public policy balance and contain appropriate limits. On this basis, the ALRC has not made any proposals in relation to s 91.1, but would consider further submissions on this point.

Secrecy provisions in other legislation

5.96 There are over 150 secrecy provisions in legislation other than the *Crimes Act* and the *Criminal Code Act* dealing with unauthorised disclosure in particular circumstances. A number of these—for example, those set out above[78]—potentially cover classified and security sensitive information. The House of Representatives Standing Committee on Legal and Constitutional Affairs noted in its report that these provisions have been criticised as being neither uniform nor consistent:[79]

---

77 Senate Legal and Constitutional Legislation Committee, *Consideration of Legislation Referred to the Committee: Provisions of the Criminal Code Amendment (Espionage and Related Offences) Bill 2002* (2002), 5.

78 See [5.41].

79 House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth* (1995), 97.

> Penalties in a number of the specific provisions are out of step with the general sentencing provisions in the Crimes Act ... Consistency in the range and expression of penalties in criminal secrecy provisions is desirable.
>
> However, the Committee notes that while consistency in penalties is desirable as an overall objective, there may need to be some flexibility depending on the sensitivity of the information to be protected ... the Committee does not consider that this need for flexibility should necessarily result in marked differences between the maximum penalties in various statutes ...[80]

5.97 While penalties across these 150 provisions vary, the secrecy provisions in the *Australian Security Intelligence Organisation Act*, the *Intelligence Services Act*, the *Inspector-General of Intelligence and Security Act* and the *Defence Force Discipline Act*, in common with s 70 of the *Crimes Act*, all carry maximum penalties of two years' imprisonment.[81] Section 51 of the *Australian Crime Commission Act 2002* (Cth), however, provides for a maximum penalty of 50 penalty units or one years' imprisonment. A further example of the lack of consistency across these provisions is s 58 of the *Defence Force Discipline Act*, which is expressly a strict liability offence, although it is limited to the disclosure of information which is likely to prejudice the security or defence of Australia.

5.98 The ALRC agrees with the concerns expressed by the Standing Committee and others about the lack of uniformity and consistency in the elements and penalty structure in this cluster of provisions, and proposes that the Australian Government initiate a review of the law in this area.

Proposal 5–5 The Australian Government should initiate a review of Commonwealth legislative and regulatory secrecy provisions to ensure that:

(a) each provision is consistent with the *Australian Constitution*, in particular, the implied freedom of political communication; and

(b) all provisions are broadly consistent, allowing for any necessary variation among agencies.

80 *Ibid*, 96–97.

81 These provisions are set out in Appendix 3.

6. Security Clearances

Contents

Introduction

6.1 The protection of classified and security sensitive information may be assisted by requiring people who are to gain access to such information during investigations and proceedings to obtain a security clearance. The rationale is that this material should only be accessed or handled by individuals with appropriate personal characteristics of reliability and trustworthiness and with an appropriate—or at least without an inappropriate—personal history that suggests that they are not a security risk. The Attorney-General's Department has explained the purpose of security clearances in these terms:

> Security clearances are preventative in nature and allow the Commonwealth to identify, as far as possible, the risk posed by allowing access to security classified information by a particular person.[1]

6.2 This issue was of significance in the *Lappas* case[2] and the Australian Government has sought changes to legal aid guidelines in relation to the representation of people charged with certain offences under amendments to the *Australian Security*

1 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
2 See Appendix 4.

Intelligence Organisation Act 1979 (Cth) (ASIO Act). A requirement for defence lawyers in cases involving classified and security sensitive information to obtain a security clearance is a controversial proposal for a number of reasons. Security clearances are a subjective and invasive process. There may be issues around who can be cleared, and they are costly and often time-consuming, potentially delaying proceedings. As well, security clearances do not fit well within the courtroom process—if all lawyers are required to be cleared, what about judges, juries and court staff?

6.3 This chapter is divided into two sections. The first examines current procedures in relation to security assessments and clearances, and how assessment and clearance decisions may be reviewed. The second section looks at the value of security clearances as a means of protecting classified and security sensitive information in court proceedings and the proposals for requiring a clearance in such cases.

How does a security clearance work?

6.4 The people dealing with classified and security sensitive information who require security clearances are generally Australian Government employees, but this requirement is also applied to contractors and others (including state and territory government employees) who need access to classified information or areas.[3] There are two categories of clearance: Designated Security Assessment Position, for positions requiring access to national security information; and Position of Trust, which is used for positions requiring access to non-national security information.[4]

6.5 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 PSM states that the number of people who need to be security cleared to perform their work should be kept to a minimum.[5] Although this may be Australian Government policy, recent reports have indicated that there has been a growth in the number of Australian Government employees requiring a security clearance, and an increase in the delay in providing these clearances.[6]

6.6 The PSM identifies the following indicators of the type of behaviour or history that might indicate whether a person is suitable to hold a security clearance: the subject's maturity, responsibility, tolerance, honesty and loyalty.[7]

6.7 The PSM acknowledges that the clearance process is discriminatory and intrusive.[8] It entails a thorough evaluation of the requirements of a specific position to

---

3 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 21, [5.1].
4 Ibid, D 17, [4.6].
5 Ibid, D 24, [5.16].
6 ABC Newsonline, *Up to 30,000 Defence Staff Awaiting Security Check*, <www.abc.net.au/news/newsitems/s939123.htm> at 4 September 2003.
7 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 30–33, [6.6–6.23].
8 Ibid, D 8, [1.7].

ascertain the level of clearance necessary, and requires the clearance, once issued, to be monitored and periodically reviewed.[9] Among the principles identified in the PSM relating to personnel security are the following:

- Security clearances should be required only where the need for access to security classified information has been clearly established.[10]

- Only people with the appropriate security clearance and a legitimate need to know may access security classified information or areas.[11]

- The procedures used to process and issue a security clearance for a person to access security classified information should be uniform.[12]

6.8 The Australian Government's clearance system is, in most cases, 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.[13] Positive vetting is generally only required for those seeking a 'Top Secret' clearance.[14]

6.9 An agency determines its need for a person to be cleared and the general criteria that he or she must satisfy. Agencies have their own processes for identifying a person's suitability for such a clearance at the initial level, and retain responsibility for determining general policies in relation to non-national security clearances and deciding whether a national or non-national clearance is required.[15]

6.10 The Australian Security Vetting Service (ASVS), which is part of the Attorney-General's Department, conducts initial clearances, clearance reviews and upgrades on a fee-for-service basis for Australian Government agencies. The ASVS conducts checks and makes recommendations. However, it does not actually determine who is suitable

---

9 Ibid, D 8, [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 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), D 55, [8.3]–[8.11]. The US Commission on Protecting and Reducing Government Secrecy has stated that most resources are directed to the initial clearance process and that 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), XXVII–XXVIII.

10 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 9, [2.3].

11 Ibid, D 9, [2.4].

12 Ibid, D 9, [2.5].

13 Ibid, D 29, [6.4].

14 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

15 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 14–15.

for a clearance or to what level. The ASVS does play a role, however, in enforcing Australian Government policy in relation to security clearances:

> The ASVS has a responsibility to contribute to a high standard of vetting across the Commonwealth. For instance, if the ASVS receives a clearance request that does not appear to justify the clearance at the level indicated from an agency, its staff will seek to clarify the need with the agency concerned before proceeding with clearance action.[16]

6.11 In 2002–03, the ASVS completed 2,896 clearances on behalf of about 60 agencies.[17]

6.12 The Australian Security Intelligence Organisation (ASIO) is the agency responsible for providing Australian Government agency heads with security assessments for employees who require access to national security information.[18] Once an agency determines that a person is suitable for access, ASIO provides a security assessment, which examines whether there is anything in the candidate's background or activities which is a cause for security concern. ASIO's advice is often based on an assessment of the material provided by the relevant agency, although ASIO conduct interviews where relevant.[19]

6.13 ASIO will then either advise the agency that it does not recommend against the candidate, or will issue an adverse or qualified assessment. An adverse assessment recommends that a person not be granted the clearance; a qualified assessment is not a recommendation against a clearance but sets out information that ASIO considers might need to be considered by the agency in deciding on clearance and to what level.[20] The agency then determines whether or not to issue the clearance.

6.14 In 2002–03, ASIO received 14,272 requests for security assessments, a 16 per cent increase on the previous year, with most clearances being sought at high levels.[21] Only two adverse and three qualified assessments were issued, which is consistent with previous years.[22]

---

16 Australian Security Vetting Service, *Fact Sheet*, <www.sac-pav.gov.au/www/protectivesecurityHome.nsf/HeadingPagesDisplay/Australian+Security+Vetting+Service?OpenDocument> at 19 August 2003.

17 Attorney-General's Department, *Annual Report 2002–03* (2003), 128. The time taken for each clearance was 47 days, down from 60 days in 2001–02.

18 ASIO's activities are described in greater detail in Ch 2.

19 Australian Security Intelligence Organisation, *Annual Report* (2002), 30.

20 Ibid, 29.

21 7,618 of the assessments requested were for 'Secret' clearances, 5,112 were for 'Top Secret': Australian Security Intelligence Organisation, *Annual Report* (2003), 29.

22 Ibid, 30.

Problems with the security clearance system

6.15 In 2001, the Australian National Audit Office (ANAO) reported on personnel security in the Australian Public Service and the management of security clearances.[23] The report concluded that Part D of the PSM provided an effective framework for the management of personnel security. However, a number of shortcomings were present in agency management of the security clearance process. The audit found that there was a significant backlog of initial clearances within many agencies, poor clearance after-care processes, and a failure to establish and enforce appropriate procedures to re-validate initial clearances within an acceptable timeframe.[24]

6.16 ANAO had previously looked at security clearances in 1999 in the course of considering the operation of the classification system for protecting sensitive information.[25] It found that a number of organisations had a very high proportion of staff with security clearances above the level that their work commitments would normally require.[26] Conversely, in other organisations the long lead times necessary to obtain a clearance meant that some staff were privy to classified information before clearances were obtained.[27]

6.17 In late 2003, the Department of Defence revealed to the Joint Parliamentary Committee of Public Accounts and Audit that around 5,000 defence employees were waiting for their first security clearance, and around 25,000 other staff needed to have their clearances checked and reviewed.[28]

6.18 In 1999, ANAO reported that the cost to an agency of obtaining a security clearance through the ASVS was $1,500 for a Top Secret clearance, $900 for a Highly Protected clearance and $600 for a Secret clearance.[29]

Review of security clearance decisions

6.19 As noted earlier, security clearances for Designated Security Assessments Positions to handle 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 (AAT).[30] This is one of the two types of matters heard by

---

23 Australian National Audit Office, *Personnel Security—Management of Security Clearances*, Report 22 (2001–2002).

24 Ibid, 3.

25 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999).

26 Ibid, 31.

27 Ibid, 31.

28 ABC Newsonline, *Up to 30,000 Defence Staff Awaiting Security Check*, <www.abc.net.au/news/newsitems/s939123.htm> at 4 September 2003.

29 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Report 7 (1999), 32.

30 *Australian Security Intelligence Organisation Act 1979* (Cth), s 54. See also Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 52, [7.10].

this Division, the other being applications under the *Archives Act 1983* (Cth) for access or partial access to an ASIO record held by the National Archives of Australia.[31] In 2002–03, the Security Appeals Division received one application for access to ASIO records, and three regarding ASIO security assessments.[32]

6.20 Other than appeal to the Security Appeals Division, the ASIO Act expressly states that no proceedings shall be brought in any court or tribunal in respect of the making of an assessment or anything done in respect of a security clearance assessment.[33]

6.21 In reviewing security assessments, the AAT conducts a private hearing[34] 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.[35] Copies of the AAT's findings are provided to the applicant, the Director-General of Security (who is the head 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 have the power to issue certificates to exempt an agency, on the basis of public interest, from providing notice of an ASIO decision to an applicant or to prevent an applicant hearing submissions.[36]

6.22 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 the making of a security assessment where that is essential for national security.[37]

6.23 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.[38] 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

---

31 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.

32 Administrative Appeals Tribunal, *Annual Report* (2003), 109. In 2001–02, the Division received one application for archive access, and eight applications regarding security assessments: Administrative Appeals Tribunal, *Annual Report* (2002), 103.

33 *Australian Security Intelligence Organisation Act 1979* (Cth), s 37(5).

34 A 'private hearing' is one where certain persons or the public are excluded from the hearing room: *Administrative Appeals Tribunal Act 1975* (Cth), s 35 and 39A. See also the discussion of hearings closed to the public in Ch 8.

35 Administrative Appeals Tribunal, *Security Appeals*, <www.aat.gov.au/leaflet8.htm> at 21 May 2003. See also the *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(5).

36 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), 4. See *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(b).

37 *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(a).

38 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.

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 they would prejudice the security or defence of Australia, the applicant (and generally the applicant's legal representative) cannot be present when the evidence is presented.[39]

6.24 As noted above, this formal review process applies only to decisions made by ASIO to provide an adverse or qualified security assessment. Even then, the normal processes of natural justice in relation to such appeals may be curtailed upon certification by either the Attorney-General or Director-General of Security, itself an unreviewable decision. Where a person is denied a security clearance based on the criteria used by an agency itself, there is no process of review or appeal.[40]

Security clearance of lawyers

6.25 There has been recent public debate about whether lawyers representing an accused charged with an offence that involves an issue of, or evidence concerning, national security should be required to have a security clearance.

6.26 Some of this debate may have been sparked by concerns arising from the trial of Simon Lappas.[41] Lappas was alleged to have tried to sell two highly sensitive documents that originated from an overseas country. That country refused to allow the documents to be tendered in open court or to allow access to them by anyone without a security clearance to the requisite level. Mr Lappas's counsel at his trial did not hold a security clearance and declined to seek one. The judge stated he had no power to force defence counsel to obtain a clearance, and eventually a confidentiality undertaking was given to the Court in order to allow access to the documents.[42]

6.27 The Australian Government has sought to introduce the requirement of counsel obtaining security clearances in two ways: through amendments to the ASIO Act and through amendments to the Legal Aid Guidelines.

6.28 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', defined as legal practitioners whom the Minister had approved and in respect of whom he or she had considered a security assessment.[43] Persons detained under a warrant[44] 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

---

39 *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(8)–(9).

40 J Renwick, *Consultation*, Sydney, 9 September 2003.

41 *R v Lappas* is outlined in detail in Appendix 4.

42 Confidentiality undertakings are considered at [6.52]–[6.53] and in Ch 8 at [8.98]–[8.117]. The undertaking given in *Lappas* is set out in Appendix 4.

43 Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill [No 2] 2002 (Cth), cl 34AA.

44 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).

the Minister was satisfied that it was likely that a terrorism offence was being committed).[45] This proposal was criticised by lawyers and civil liberties groups.

6.29 In June 2003 the Government proposed changes to the ASIO Bill relating to access to a lawyer, replacing it with a scheme that provided for the provision of a lawyer of choice. Following passage of the Bill, the ASIO Act now provides that a detained person's lawyer does not have to hold a security clearance. However, regulations 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 he or she be security cleared.[46] However, the lack of access to classified material could well restrict the lawyer's ability to represent the detained person effectively.

6.30 In January 2003, the Australian Government proposed changes to the availability of legal aid in national security matters:

> 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.[47]

6.31 Under these proposals, defendants would not receive legal aid to instruct or brief uncleared lawyers to act in a 'matter relating to Australia's national security'. The Government's proposal and the Legal Aid Guideline that ultimately came into effect do not define a 'matter relating to Australia's national security', nor who declares a case to fall within this category. In many cases, it may be very clear whether it is in fact a matter relating to Australia's national security. However, if the decision whether any particular case is a matter relating to Australia's national security rests with a government officer, the executive government has the power to determine when a lawyer must seek a clearance and when in fact he or she will get it.[48]

6.32 The Government's proposals attracted criticism from lawyers and civil liberties groups, in particular because the proposed rules were contrary to an important principle covering the provision of legal aid—that its recipients are to be treated in exactly the same manner, in terms of their legal representation, as clients who pay for their own lawyers.[49] The ALRC understands that the Government's intention was not to distinguish legal aid lawyers from other lawyers, and the Government would seek to extend

---

45 Ibid, cl 34C(3B) and (3C).

46 Office of the Attorney-General, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002—Government Proposals*, 11 June 2003.

47 The then Attorney-General, the Hon Daryl Williams AM MP QC, outlined the proposal in a letter to state attorneys-general. See F Wilkins, 'National Security and the Legal Aid Rules', *Lawyers Weekly*, 7 February 2003, 10; I Munro, 'Suspects' Lawyers in Line for Security Check', *The Age* (Melbourne), 10 February 2003.

48 The Government has not given a clear indication of how a matter will be defined as involving matters of national security. A spokeswoman for the Attorney-General has stated that the term 'national security' would apply to terrorism and espionage cases: I Munro, 'Suspects' Lawyers in Line for Security Check', *The Age* (Melbourne), 10 February 2003.

49 F Wilkins, 'National Security and the Legal Aid Rules', *Lawyers Weekly*, 7 February 2003, 10.

its proposals ultimately to all lawyers participating in cases involving classified or security sensitive information. It appears that it was only the Government's ability to quickly implement policy changes in regard to legal aid lawyers that meant that they were the first to be affected.

> 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.[50]

6.33 The Law Council of Australia argued that, if a particular lawyer represented cause for concern in relation to their handling of classified information, then the issue should be brought before a judge, who could impose the appropriate restrictions.[51]

6.34 The NSW Law Society's Criminal Law Committee 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.[52]

6.35 The President of the NSW Council for Civil Liberties 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.[53]

6.36 As an interim measure, the Australian Government promulgated this additional requirement in the Commonwealth Legal Aid Guidelines, effective from 27 August 2003.

Overseas examples of clearance requirements for lawyers

6.37 A requirement that lawyers appearing in matters involving classified information have an appropriate security clearance is part of the regime for protecting classified and security sensitive information in a number of overseas jurisdictions.

6.38 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:

---

50 Ibid, 10.
51 Ibid, 10.
52 'Opposition to Security Clearance Requirement for Legal Representatives' (2003) 41(2) *Law Society Journal* 6.
53 C Banham, 'If National Security's in Peril, So Is Legal Aid', *The Sydney Morning Herald*, 25 January 2001, 3.

> 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.

6.39 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'.[54] This requirement presumably extends to lawyers (and other people) involved in any case covered by 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.[55]

6.40 The security procedures established under 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.[56]

6.41 There has been some confusion in the United States over whether the CIPA provisions mean that defence counsel can be compelled to obtain a security clearance. Earlier cases suggested that the courts could not.[57] However, in *United States v Bin Laden*,[58] the US District Court disagreed and held that CIPA permitted a judge to resolve issues about clearances, and ordered defence counsel to obtain a clearance.

6.42 The US Department of Justice has drafted further anti-terrorism legislation in the form of the proposed *Domestic Security Enhancement Act 2003*, also known as PATRIOT ACT II (draft).[59] Section 108 of that Act would amend the *Foreign Intelligence Surveillance Act 1978* to permit the Foreign Intelligence Surveillance Act (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 US Government appeals a ruling to the FISA Court of Review.[60]

---

54 Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam>, 2054.

55 Ibid, 2054.

56 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.

57 See for example, *United States v Jolliff* 548 F Supp 227 (DMd, 1981) and *United States v Smith* 706 F Supp 593 (MD Tenn. 1989).

58 *United States v Bin Laden* 58 F Supp 2d 113 (SDNY, 1999).

59 A copy of the draft legislation can be found at <www.dailyrotten.com/source-docs/patriot2draft.html>.

60 The Foreign Intelligence Surveillance Court is discussed in Ch 9.

6.43 The US Military Rules of Evidence authorise a military judge, at the request of the US 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.[61] There is also the possibility that an accused might deliberately choose civilian or military counsel whom he or she knows will not be cleared, in order to delay or derail proceedings.[62]

6.44 More recently, Legal Instructions have been issued for the trial of detained individuals by US Military Commissions if the US President names individuals to be considered for prosecution.[63] 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.[64] 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.

6.45 In Canada, independent security-cleared counsel appear before hearings conducted by the Security Intelligence Review Committee (SIRC).[65] 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.

---

61 C Maher, 'The Right to a Fair Trial in Criminal Cases Involving the Introduction of Classified Information' (1988) 120 *Military Law Review* 83.

62 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 (DMd, 1981), 233, the court stated that 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 Appeals 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 US 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. The text of the Sixth Amendment to the US Constitution is set out in Appendix 3.

63 J Porth, *DOD Legal Officials Ready Rules for Future Military Commissions*, 2 May 2003.

64 Department of Defense (USA), *Military Commission Instruction No 5*, 30 April 2003, 2(d).

65 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* RS 1985, c C-23 (Canada), s 38; and I Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113.

> … without knowledge of CSIS's evidence, counsel to the complainant faced inevitable difficulties in preparing for this vicarious cross-examination.[66]

Status of Australian lawyers

6.46 Is there any basis in principle for asserting that lawyers as a group should be exempt from security clearances to which public servants (and some others involved in court proceedings) are subject if they are to obtain access to classified or security sensitive information? Two points of distinction are that lawyers must be held to be of good fame and character in order to be admitted to practise and are bound by their duties as officers of the court.

6.47 BP 8 asked about the sufficiency of measures currently in place to determine whether an applicant for admission to practice as a solicitor or barrister is a 'fit and proper person of good character'—or whether the vetting processes 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 or acts of bankruptcy.[67] Applicants 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.

6.48 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.'[68] 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.'[69] 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.'[70] 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.'[71]

---

66 I Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113, 163.

67 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.

68 *Legal Practice (Admission) Rules 1999* (Vic), r 4.01(1)(c).

69 Ibid, r 4.13.

70 *Legal Practice (Admission) (Amendment) Rules 2003* (Vic), r 1.

71 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

6.49 The Standing Committee of Attorneys-General has proposed the development of a nationally consistent regulatory regime for the legal profession. A Model Bill has been prepared for the purposes of consultation. 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.'[72] 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;[73] …
>
> (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;

---

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* (Vic) 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.' See also *Legal Practitioners Rules* (NT), s 7–9, and *Supreme Court (Admission of Legal Practitioners) Rules No 15 1998* (ACT), r 11, 13 and 15.

72 Parliamentary Counsel's Committee, *Legal Profession—Model Laws Project—Consultation Draft*, 6 May 2003, cl 301(1).

73 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.

> (k) whether the person is subject to an order under this Act[74] 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; …[75]

6.50 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.

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

6.52 In addition to the rules of admission, lawyers are also bound by the conventions and rules of the court in which they practice. For example, parties to any litigation are subject to an implied undertaking to the court not to use or disclose information they receive through the court's compulsory processes,[76] except for the purpose of those proceedings, without the leave of the court or the consent of the originator of the material. A breach of such an undertaking may be punishable as contempt.[77] These undertakings are considered in more detail in Chapter 8.

6.53 A number of court rules allow the court to punish breaches of express or implied undertakings to the court. For example, the Federal Court Rules provide that, where a person (whether a party or not) fails to fulfil a binding undertaking to the Court to do or refrain from doing any act or to pay any sum of money, following a motion by any party to enforce the undertaking, the Court is to make the order that the person do or refrain from doing the undertaken act or pay the sum of money.[78]

---

74 The name of the proposed Act is the *Legal Practitioners Act 2003:* Ibid, cl 101.

75 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.'

76 Such as discovery, subpoenas and orders for witness statements.

77 Australian Government Solicitor, *Legal Briefing Number 56: Contempt of Court—How it Can Affect You*, <www.ags.gov.au/publications/briefings/br56.html> at 25 June 2000.

78 *Federal Court Rules 1979* , O 35, r 11. See also Ch 8 at [8.109].

Submissions and consultations

6.54 In a submission to the ALRC, the Law Council of Australia raised an important threshold question—what is the problem that the introduction of a system of security clearances is thought to solve?[79]

6.55 The Australian Government has argued that it is an established part of Commonwealth protective security policy that national security documents can only be accessed by people who hold a security clearance. Importantly, this policy is consistent with the policies of other countries with whom the Australian government exchanges security and intelligence information.[80] Under Article Four of the *Agreement between the Government of Australia and the Government of the United States of America Concerning Security Measures for the Protection of Classified Information*,[81] Australia and the United States have agreed to disclose, release or provide access to classified information received from the other party only to individuals who require such information and who hold an appropriate personnel security clearance. Australia has similar protocols in place with other countries with which intelligence information is shared.

6.56 It was emphasised in submissions and consultations that relations with allies was a key reason for the Government seeking to require defence counsel to have a security clearance in cases involving classified and security sensitive information.[82] If the lawyers in a criminal proceeding involving matters of national security are not cleared, a trial may be significantly affected, restricted or even abandoned.

6.57 The Attorney-General's Department has noted that lawyers who act for the Commonwealth and who have access to classified information are required to obtain a security clearance and, therefore:

> There is no reason why lawyers acting for the defendant should be given access to security classified information on any basis other than that also applicable to the lawyers for the Commonwealth.[83]

6.58 However, these lawyers are often briefed or instructed repeatedly by the Government and have strong professional incentives for being cleared. The same cannot necessarily be said of defence counsel or lawyers acting for non-government parties.

---

79 Law Council of Australia, *Submission CSSI 11*, 12 September 2003, 19.

80 The Hon Daryl Williams AM QC MP, *States and Territories Fail to Support Safeguards for National Security*, Media Release, 11 April 2003.

81 *Agreement between the Government of Australia and the Government of the United States of America Concerning Security Measures for the Protection of Classified Information*, 25 June 2002, Australia and United States of America, [2002] ATS 25, (entered into force on 7 November 2002).

82 Attorney-General's Department, *Consultation*, Sydney, 19 June 2003; Commonwealth Director of Public Prosecutions, *Consultation*, By telephone, 3 November 2003; Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

83 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

6.59 The Victorian Bar has argued 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.[84]

6.60 Many of the concerns expressed to the ALRC related to the singling out of legal aid lawyers as having to obtain clearances although, as discussed above, this was not the express intention of the Government. National Legal Aid (NLA) expressed a number of concerns with the new guidelines. Firstly, there is an implication that the Government is interfering in the independence of the legal profession. As well as prosecuting a case, one branch of the government or another will be responsible for authorising the appropriate national security clearance. The decision to grant or not grant a clearance may well be subject to both internal and external appeal from the appropriate government decision-maker.[85] In addition, the process of requiring lawyers to obtain security clearances could interfere with a client's ability to nominate a lawyer of choice to act for him or her. If the lawyer is not prepared, or is unable, to obtain a security clearance, that lawyer will not be able to undertake a matter for a client in a court where he or she is otherwise able to practise.[86]

6.61 Victorian Legal Aid (VLA) submitted that the requirement for security clearance for lawyers will seriously affect its ability to provide adequate and proper services and will unfairly discriminate against individuals who are unable to instruct a legal practitioner of their choice. Further, the proposed security clearance requirement has the capacity to prejudice the independence of the private profession because it may require members of the private profession with legally assisted clients to be vetted by Government. VLA argues that establishing a special class of lawyers for those requiring legal aid in national-security-related trials is offensive in principle, stigmatises those lawyers and clients, and requires lawyers to participate in an unnecessarily intrusive process of security vetting. Finally, VLA cautioned that a security clearance requirement may alienate those members of the legal profession who are currently prepared to do legal aid work.[87]

6.62 The Victorian Bar has raised the issue of who will pay for a security clearance of defence lawyers. The Australian Government has not given a clear indication on this issue generally, although in the case of legal aid lawyers, the Commonwealth will pay for the cost of the clearance out of its legal aid funding.[88] In its submission, VLA expressed concern that existing legal aid funds would be used to implement this system.[89]

---

84 The Victorian Bar, *Submission CSSI 1*, 8 April 2002.
85 National Legal Aid, *Submission CSSI 8*, 3 September 2003.
86 Ibid.
87 Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003.
88 The Hon Daryl Williams AM QC MP, *States and Territories Fail to Support Safeguards for National Security*, Media Release, 11 April 2003.
89 Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003.

6.63 The Victorian Bar also questioned who would be charged with determining whether a matter relates to national security?[90] They argued that there is uncertainty as to who would decide whether a case was a 'national security matter' and on what basis. There was no indication that such a decision would be subject to review and the lawyer in question would be in no position to debate the matter because he or she would not have had access to the relevant documents.[91]

> 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.[92]

6.64 The NSW Bar Association accepted that in some 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'?[93]

6.65 Would a security clearance requirement derogate from the principle that a person should be able to be represented by a lawyer of his or her own choice? The NSW Bar Association submitted that:

> 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 [would] 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.[94]

6.66 These comments were echoed by the Law Society of NSW in opposing the Legal Aid Guideline on the basis that:

---

90 See also [6.31] above.
91 The Victorian Bar, *Consultation*, Melbourne, 26 May 2003.
92 The Victorian Bar, *Submission CSSI 1*, 8 April 2002.
93 New South Wales Bar Association, *Submission CSSI 2*, 11 April 2003.
94 Ibid.

> it would impose an arbitrary and unacceptable limitation on the right of people to be represented by the lawyer of their choice.[95]

6.67 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.[96]

> 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.[97]

6.68 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.[98] The principles might also apply where an indigent person 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* principles 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.

6.69 However, a right to counsel is not the same issue as a right to be represented by a lawyer of choice. Much of the Australian case law in this area concerns the right of a party to be represented by counsel who may be seen to have an unfair interest in the proceedings, or who may give rise to a concern that the integrity of the judicial process would be lost. In *Macquarie Bank Ltd v Myer*, Marks J found that:

---

95 'Opposition to Security Clearance Requirement for Legal Representatives' (2003) 41(2) *Law Society Journal* 6.

96 *Dietrich v The Queen* (1992) 177 CLR 292, [40].

97 Ibid, [40].

98 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).

> The court will be slow to interfere with the prima facie right of a litigant to choose his, her or its solicitors. If the court is to interfere, it is only to protect the undue risk of unfairness or disadvantage which the circumstances might reveal to exist.[99]

6.70 *State of Western Australia v Ward* concerned whether counsel could be restricted from hearing certain evidence relevant to a native title claim on the basis of gender. Hill and Sundberg JJ (Branson J dissenting) found that:

> A court exercising federal jurisdiction, like any other court, must if it be necessary to ensure that justice be done and be seen to be done, and thus, that the integrity of the judicial process be protected, have the power to prevent a particular counsel or solicitor from appearing for a party.[100]

6.71 The majority stated that the public interest in the ability of a litigant to have a lawyer of its choice may require some modification where there is an overriding public interest in ensuring a fair trial.[101] In the facts of that case, this meant that, while orders resulting in lawyers of one gender receiving certain information not available to the lawyers of the other gender would be undesirable and impact on the right to counsel of choice, justice (in these particular circumstances) was better served by allowing the applicants to give evidence which, by virtue of their spiritual beliefs, could only be revealed to persons of the same gender.[102]

6.72 It should also be borne in mind that the right to counsel of choice is restricted in practice by issues such as availability, cost, conflict of interest and so on. In any event, as a matter of practicality, the right to the effective assistance of counsel does not necessarily extend to the right to demand representation by the most senior or experienced lawyers in the profession, especially in relatively minor cases.

6.73 While not directly analogous, courts could take a similar approach to the issue of security clearances. If, as was the case in *Lappas*, evidence could not be presented to the defence because counsel lacked a security clearance, the courts may take the view that the interests of justice require that counsel be security cleared and order that they seek such a clearance or at least that certain information can only be shown to counsel and other people who hold a particular clearance.

6.74 As well as its general philosophical opposition to security clearance requirements for lawyers, the Law Council of Australia suggested a number of practical problems. One example given was the unexpected emergence of classified information in the course of proceedings in a trial conducted by non-cleared lawyers. Would the trial have to be aborted or stayed until security-cleared defence counsel can be found or existing counsel obtained clearance.[103]

---

99 *Macquarie Bank Ltd v Myer* [1994] VR 350, 352.
100 *State of Western Australia v Ward* (1997) 145 ALR 512, 513.
101 Ibid, 519.
102 Ibid, 519.
103 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

6.75 The Law Council has pointed out that the review procedures available in the Security Appeals Division of the AAT, discussed above, may be inadequate if lawyers must be cleared for certain cases. The Law Council argues that defence counsel may be unaware that clearance is required for a particular case, or unaware that he or she has been the subject of an assessment, although it is not clear in what circumstances this might occur. As noted above, if the lawyer were unable to be cleared due to a finding of the Australian Security Vetting Service or any agency other than ASIO, no avenue of appeal would be available. The Law Council submitted that this gives the Government an unreviewable decision that in part determines who may or may not appear in cases involving classified and security sensitive information.

6.76 VLA submitted that there are already sufficient stringent requirements to ensure that lawyers are competent to operate in sensitive areas of national security, and are answerable for contraventions of this duty, noting the *Legal Practice Act 1996* (Vic) and the *Legal Practice (Admission) Rules 1999* (Vic) and the professional practice rules administered by the Law Institute of Victoria and the Victorian Bar.[104]

6.77 One view put to the ALRC is that a comparison cannot be made between national security information and other types of information which may be protected in proceedings by undertakings, such as commercial information. It is argued that national security and intelligence gathering is a highly specialised field of understanding. All government staff who deal with it are required to hold a security clearance. There is no reason why the legal profession should not conform to a 'more rigorous qualification process, specifically devised for minimising risks of compromise of classified information, as and when practitioners are required to deal with such material'.[105]

6.78 The Attorney-General's Department agrees with this position, submitting that:

> The current process used for admission as a barrister or solicitor does not appear sufficient to justify exempting these people from undergoing the clearance vetting process. For example, practising lawyers in the Commonwealth public service are not given access to security classified material until the vetting process assesses them as being suitable. It must also be noted that the admissions process is based on information obtained only at the time of admission and there is no process for systematic and subsequent review.[106]

6.79 The Attorney-General's Department also notes the educative role of the security clearance process:

> Undergoing a security clearance process also offers the Commonwealth the opportunity to educate people who require access to classified material on the proper treatment of that material. People who are not usually exposed to classified material are,

104 Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003.
105 Advisory Committee member, *Correspondence*, 18 September 2003.
106 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

understandably, unfamiliar with the proper protection of that material and are at risk of compromising material unwittingly.[107]

Commission's views

6.80 A security clearance does not of itself guarantee that information is safe from improper disclosure. Indeed, it is not facetious to say that, when national security information has been disclosed unlawfully, it is usually at the hands of someone with a high-level security clearance—since these are by definition the people with access to such information. On the other hand, requiring a security clearance is an essential feature of sensible risk management in that it helps to prevent people who are discerned to be security risks from having contact with the information.

6.81 Security clearance requirements do not deal with the issue of complacency. The protection of classified and security sensitive information may be more effective on a case-by-case basis by the giving of specific undertakings because they are focussed on the specific protective measures required in relation to specific material. It could be a mistake to believe that, simply because someone is security-cleared, there is no need to be concerned about their handling of the material. This view was echoed in consultations: it was said that undertakings were specific to the case in question and were entered into by people mindful of what should be protected in the particular circumstances of that case. A security clearance, it was said, did not do anything to actually protect documents.[108]

6.82 However, clearances and secrecy undertakings serve different purposes. A security clearance goes to the character of the individual concerned and filters out people who might be unreliable. Undertakings relate to specific obligations in specific circumstances. See Proposal 10–23 in relation to confidentiality undertakings in Chapter 10.

6.83 The ALRC has concluded that the background checks on lawyers required for admission to practise provide no real substitute for security clearance processes undertaken for the purposes of clearing people to handle classified and security sensitive information. They provide no reason why lawyers should not be subject to security clearances in particular cases.

6.84 It is not a novel concept to impose additional requirements on lawyers and other professionals in order for those professionals to carry on a particular aspect of their profession. For example, lawyers who wish to hold themselves out as having specialist accreditation must meet certain criteria.[109] The need for further or special qualifications

---

107 Ibid.

108 The Victorian Bar, *Consultation*, Melbourne, 26 May 2003.

109 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 accredi-

also applies to other professions. People who carry on a financial services business must hold a financial services licence, subject to some exceptions.[110] Accountants must be licensed to give specific advice on superannuation.[111]

6.85 The ALRC accepts that there are some practical problems associated with the requirement to obtain a security clearance. 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 whom the accused has approached had been refused—or refused to seek—a security clearance, or there would be undue delay associated with the lawyer obtaining the relevant security clearance.[112]

6.86 National Legal Aid has raised the issue of delay as a key concern:

> Even if the lawyer was prepared to undergo the process of obtaining a national security clearance the question arises of how long that process will take and what other arrangements would be available to clients in areas where there were no other lawyers with the appropriate clearance.[113]

6.87 However, if this problem arises in practice—particularly early in the proceedings, as the Proposals in Chapter 10 would encourage—the court could make such orders that it saw fit in relation to the legal costs and other costs associated with the clearance process and in relation to any necessary adjournment of the matter.

6.88 In Chapter 10, the ALRC proposes the enactment of a statute setting out a procedural framework for the disclosure and admission of classified and sensitive national security information in court and tribunal proceedings. One purpose of this new Act would be to ensure that courts and tribunals have a flexible system at their disposal to allow them to deal with situations dealing with classified and security sensitive information. The ALRC has formed the preliminary view that allowing courts to order that counsel appearing in a matter involving classified and security sensitive information obtain a security clearance to the relevant level is an appropriate part of such a system. Since, in principle, there should be no distinction between legal aid and

---

ted specialists must renew accreditation annually and undergo ongoing specialist legal education to retain their accreditation.

110 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.

111 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.

112 The Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), D 27, [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: '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.

113 National Legal Aid, *Submission CSSI 8*, 3 September 2003.

any other lawyers in relation to security clearances, the Legal Aid Guideline introduced as an interim administrative measure would be replaced by the broader discretion of the court to make an order.

6.89 Under the Proposals in Chapter 10, a court may make orders for the use of classified or sensitive national security information, including restrictions on the people to whom any classified or sensitive national security information may be given or to whom access to that information may be given, such as requiring that a party or its legal representatives obtain any security clearance. The court may consider these issues on the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion. Thus, under this proposed scheme, the courts retain the ultimate discretion to determine the procedures that will apply in any particular case in line with the dictates of justice. In cases where a clearance cannot be obtained, and the defendant or party to proceedings will be substantially disadvantaged, the court may choose not to grant the order sought.

6.90 This would also deal with the issue of determining when a matter 'relates to Australia's national security'. Whilst the Attorney-General could make submissions on this topic, it would be for the court, not the executive government, to determine when counsel appearing before it require security clearances.

6.91 A requirement imposed by the court—in the light of submissions from a government agency that is party to the case, or by the Attorney-General of Australia intervening—that any lawyers who access classified or sensitive national security information seek the appropriate security clearance, or that certain material only be shown to people (whether lawyers or not) with an appropriate clearance, would allow Australia to meet its domestic concerns about the protection of such information as well as its international obligations regarding shared intelligence. Such a requirement would also ensure that all legal representatives in a case are treated equally.

Proposal 6–1 The Legal Aid Guideline requiring lawyers receiving legal aid funding in matters relating to Australia's national security to be security cleared should be rescinded.

Security clearance of judges and magistrates

6.92 If it is thought appropriate that lawyers be required to hold the necessary level of clearance to view classified documents, should judges and magistrates also be required to obtain security clearances in similar circumstances? There are some obvious and fundamental objections to any such proposal. The idea that the executive government could vet judges or magistrates and select who would sit on a court or in a particular case based on a secret security assessment of some sort closed to public scrutiny strikes at the heart of the notion of the separation of powers—which is central to the *Australian Constitution*—and at the independence of the judiciary and magistracy.

6.93 No security clearance is currently required for any Australian judge or magistrate. Neither is any security clearance required for judges in the USA under CIPA, 'but such clearance shall be provided upon the request of any judicial officer who desires to be cleared'.[114]

6.94 The Law Council of Australia submitted that a system of security clearances for judges issued by a federal agency would not withstand constitutional challenge:

> Chapter III judges are chosen exclusively from the ranks of lawyers, and if the selection process was in any way tainted by the question whether a particular appointee was or was not a security cleared lawyer, it is not hard to see an argument based on a *perception* that, in view of the role of the executive in the direct selection of judges, the judiciary is not fully independent of the executive.[115]

6.95 The Law Society of NSW agrees:

> A requirement that only those judges and magistrates who have been subsequently 'security cleared' can deal with cases involving classified and security sensitive information would adversely impact on judicial independence, be contrary to the principle of the separation of powers doctrine, undermine confidence in the judiciary and would be totally inappropriate and unacceptable to the community.[116]

6.96 The Law Society of NSW also notes that there is already some limited 'vetting' of judges and magistrates as part of their appointment for office to the extent that the usual consultations would highlight issues of character and personal and professional integrity.[117] However, there is no equivalent in Australia of the extensive Senate confirmation hearings conducted in the US, with respect to all nominees for federal judicial appointment.

6.97 Apart from matters of basic principle, there would also be practical concerns about a move in this direction. 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.

Commission's views

6.98 The Australian Government has not expressed any intention to require judges and magistrates to be security cleared as part of the proposals regarding clearance of lawyers. As well, there has been no support for such a proposal amongst participants in the inquiry to date.

---

114 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.

115 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

116 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

117 Ibid.

6.99 The ALRC agrees that there are important concerns with such a proposal related to the separation of powers.[118] Allowing the executive to investigate judges and security clear them, thus controlling the pool of judges who could be allocated to cases involving national security, would have an unacceptable impact on judicial independence. The risk-management purpose of a security clearance is not relevant in the case of judges (as opposed to other members of the legal profession) as, by virtue of their position of trust, they have been designated as people of high integrity, able to receive and protect highly secret information.

6.100 It is the therefore the ALRC's strong view that judges and magistrates should not be subject to any security clearance in relation to their duties.

Security clearance of other participants in court proceedings

6.101 The question also arises whether others involved in the court process, apart from lawyers, should be required to obtain a security clearance in matters involving classified and sensitive national security information. This could include jurors, court staff, court reporters, translators and others.

Jury members

6.102 BP 8 asked whether members of juries should be required to undergo a security clearance process in matters involving classified and security sensitive information.[119] This is not presently the case in Australia.

6.103 While not seeking clearances, in the trial for espionage of Brian Regan in the US, jurors were asked to fill out a detailed questionnaire revealing their thoughts about crime, espionage, the terrorist attacks on 11 September 2001 and the death penalty.[120]

6.104 In the UK, the *Juries Act 1974* allows for jury vetting in accordance with guidelines issued by the Attorney-General. The principles that are generally to be observed when utilising this procedure are:

(a) that members of a jury be selected at random from a panel;

(b) that no class of persons other than those specified as disqualified or ineligible for service in the *Juries Act 1974* together with the *Juries Disqualification Act 1984* may be treated as disqualified or ineligible; and

(c) the correct way for the Crown to seek to exclude a member of the panel from sitting as a juror is by the exercise in open court of the right to request a stand by or, if necessary, to challenge for cause.

---

118 See *Kable v Director of Public Prosecutions (NSW)* (1996) 189 CLR 51.

119 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 78.

120 'Spy Trial May End in Death', *The Canberra Times*, 15 January 2003, 11.

6.105 One view is that the usual constraints on jurors regarding the confidentiality of their deliberations and any other constraints arising from an in-camera hearing are insufficient to address the security risks raised by placing highly classified documents in the hands of jurors.[121]

6.106 However, the view has also been put that it is difficult to see how security vetting of jury members could take place without defeating the objective of having a jury of an accused's peers chosen at random—as required in federal matters by s 80 of the *Australian Constitution*. In order to obtain a sufficiently high-level clearance, jurors would have to agree to an intrusive vetting process. This agreement or otherwise could of itself constitute a selection factor that would lead to the selection of jurors of a certain disposition, even before the security clearance was undertaken.[122] However, it has also been argued that jury-vetting is not incompatible with s 80.[123]

6.107 The security procedures established in the US 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'.[124] 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.[125]

6.108 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.[126]

---

121 Advisory Committee member, *Correspondence*, 18 September 2003.

122 Ibid. Section 80 reads: 'The trial on indictment of any offence against the law of the Commonwealth shall be by jury …' See also Appendix 3 and discussion in Ch 7 under the heading 'The right to trial by jury'.

123 J Stellios, 'Section 80 of the Constitution—"A Bulwark of Liberty?"' (Paper presented at The Australian Constitution in Troubled Times, Canberra, 7–9 November 2003), 89. See Ch 7, fn 102.

124 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.

125 Ibid, point 6.

126 See the proposed *Domestic Security Enhancement Act 2003* (PATRIOT ACT II), s 206.

6.109 In relation to the operation of the CIPA provisions, the ALRC has been advised that the cautionary instruction given to jurors has worked well in practice. There have been no known cases of juror disclosure in matters involving national security.[127]

6.110 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.[128] This could create some pressure to move towards trials without juries, although there is strong support for juries in federal criminal matters and, under s 80 of the *Australian Constitution*, it is not possible to exclude a jury in relation to federal indictable offences.

Court and tribunal staff

6.111 Concerns have been raised with the ALRC regarding the training and experience of court and tribunal staff in dealing with matters involving classified and security sensitive information. In particular, court staff who deal with the transcripts of closed court or tribunal proceedings may be in possession of highly sensitive information. The ALRC has been told that, chiefly because such cases rarely arise, staff may be unaware of the appropriate security procedures.[129]

6.112 Under CIPA, 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 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.[130]

6.113 In *United States v Smith*,[131] the US Court of Appeals (6th Circuit) upheld the CIPA procedures that require court personnel to undergo security clearances, and held that such provisions did not violate the principles of the separation of powers.

6.114 The NSW Law Society has argued that there is a case for court staff to be security cleared in certain circumstances.

---

127 United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003.

128 The Victorian Bar, *Submission CSSI 1*, 8 April 2002.

129 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003.

130 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.

131 *United States v Smith* 899, F 2d 564, 570.

> It may be appropriate, however, for staff, such as court attendants and court reporters involved in court and tribunal proceedings who are not lawyers and hence, apart from their employment or contractual obligations, do not have a professional responsibility to the court, to be subject to requirements of appropriate security clearances, the cost of which should be met by the court or tribunal concerned but which should be funded through the normal budget processes.[132]

Commission's views

6.115 The ALRC agrees that there are a number of problems of principle and practice inherent in any suggestion that jurors submit to security clearances. In particular, the argument outlined above, that such a requirement would lead to a self-selection process, is persuasive. In *Brownlee v R*, Gleeson CJ and McHugh J identified independence, representativeness and randomness of selection as some of the essential attributes of a jury trial.[133]

6.116 For these reasons, the ALRC proposes that there not be any requirement that jurors sitting on matters involving classified and security sensitive information seek a security clearance.

6.117 The adoption of the other recommendations outlined in Chapter 10 below—principally Proposals 10–10(b)(vii) and 10–21—would also alleviate the need for requiring jury members to obtain clearances, as it would allow classified and security sensitive information to be protected from uncleared persons (including jurors) in a number of other ways in court proceedings, such as through redaction.

6.118 However, the ALRC views the position of other court and tribunal staff as more directly analogous to other public service employees than, for example, lawyers. The ALRC considers it is appropriate that court and tribunal staff placed in a position to view or deal with classified and security sensitive information be cleared to the correct level, if the court or tribunal so requires. Such clearance procedures will also ensure that staff are trained and aware of the security issues associated with the protection of such information.

6.119 Under CIPA, the assignment of court security officers or case managers is specifically provided for in the Guidelines prepared by the Chief Justice of the United States.[134] The use of such a case manager is discussed in greater detail in Chapter 8 at [8.71]–[8.75] and in Chapter 10—see Proposal 10–36. A key part of such a person's function could be to advise the court of the need for court staff to obtain an appropriate security clearance to deal with the case.

---

132 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003. The Attorney-General's Department has also expressed support for this proposal: Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

133 *Brownlee v R* (2001) 207 CLR 278, 289.

134 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, [2].

6.120 The ALRC therefore proposes that, on the application of any party to the proceedings or the Attorney-General of Australia intervening, or on its motion, the court may order that any specified person (including court staff, court reporters and interpreters), seek a security clearance to a specified level appropriate to the classified or sensitive national security information used in the proceedings. The court may also make orders about who shall bear the costs of any such clearance. Alternatively, the court may order that specified material not be disclosed to any person who does not hold a security clearance at a specified level. This proposal is included as part of the new Act dealing with the protection of classified and security sensitive information contained in Chapter 10. See Proposal 10–24.

Proposal 6–2 There should be no requirement of any sort imposed by the executive government that any judge, magistrate or juror be security cleared before participating in any case.

Sector-specific clearances

6.121 In BP 8, the ALRC noted that threats of terrorism have brought the security of critical infrastructure to the fore, and that partnerships were proposed between the private and public sectors to manage information. The Australian Government acknowledged the significant role that the private sector has to play in managing the new security environment,[135] launching the Trusted Information Sharing Network for Critical Infrastructure (TISN) in April 2003. 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.[136]

6.122 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.[137]

6.123 The Attorney-General's Department has stated that the same standards set out in the PSM used to vet and grant security clearances to Commonwealth officials are used

135 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).

136 The Hon Daryl Williams AM QC MP, *Protecting Our Critical Infrastructure*, News Release 35/03, 2 April 2003.

137 D Goodsir, 'ASIO to Give Terror Secrets to Business', *The Sydney Morning Herald*, 26–27 April 2003, 3.

in security clearance vetting for contractors and non-Government employees.[138] In short, no special procedures are to apply.

6.124 In the light of these assurances, the ALRC does not propose to make any further comment on these matters.

138 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

PART C

Classified and Security Sensitive Information in Court

7. Principles of Open Justice and Fair Trials

Contents

Introduction

7.1 Principles of open justice and the minimum requirements of a fair trial should be considered when assessing actual or potential methods used to restrict disclosure of classified and security sensitive information in court and tribunal proceedings. Rights in relation to a public hearing are qualified,[1] but certain rights in international law in relation to a fair trial have been held to be non-derogable.[2] There will inevitably be some tension between the rights expressed in Australian and international law in relation to a public and fair hearing, and the operation of existing or proposed mechanisms designed to protect classified and security sensitive information.[3] Legislative provisions enabling the closure of courts to the public may 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 conflict with a person's right to be tried

1 The right to a public trial expressed in Art 14(1) of the International Covenant on Civil and Political Rights (ICCPR)—set out at [7.7] below and in Appendix 3—and in s 80 of the *Australian Constitution* is not absolute.

2 See fn 70 below.

3 Methods used to restrict disclosure of such information are discussed in Ch 8 and Ch 9.

in his or her presence and to have the opportunity to examine the witnesses against him or her.

7.2 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) may be distinguished from those in which such information is incidental. Obviously, the public interest in protecting such information by avoiding or limiting its disclosure, and the right of an individual to a fair hearing, are more acutely at odds where classified or security sensitive information is central to the indictment.

7.3 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 this information 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.

7.4 Prosecutions involving military and intelligence personnel are more likely to fall into the category of cases in which the defendants are privy to classified or security sensitive information in the possession of the state.[4] Historically, it is in these types of cases that defendants have made greymail threats to divulge classified information during the course of a trial. The greymailing defendant presents the Government with the dilemma of either disclosing 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 …[5]

The right to a fair hearing

7.5 There are a number of key principles encompassed within the broad concept of a fair hearing, although none are absolute rights and all may be qualified in some way in certain circumstances. These principles include a person's right to a public hearing; the right to certain minimum procedural protections, such as being fully informed of the

---

4 An 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>.

5 L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), 292. According to Lustgarten and Leigh (at 292), 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.

case against him or her; the right to 'equality of arms' between the parties to the case; and the right to a full statement of the reasons for any decision or judgment. Each of these matters is addressed in this Chapter.

The right to a public hearing

7.6 It has been said that:

> The right to a public hearing means that not only the parties in the case, but also the general public, have the right to be present. The public has a right to know how justice is administered, and what decisions are reached by the judicial system.[6]
>
> Courts must make information about the time and venue of the oral hearings available to the public and provide adequate facilities, within reasonable limits, for the attendance of interested members of the public.[7]

7.7 The International Covenant on Civil and Political Rights (ICCPR), which is binding on Australia,[8] 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.[9]
> [emphasis added]

7.8 Article 14(1) applies to both criminal and civil proceedings, and arguably also to administrative proceedings.[10] As the ICCPR allows for the closure of courts for

---

6 Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, [14.1].

7 Ibid, [14.2] (citations omitted).

8 The ICCPR was ratified by Australia in 1980. In 1991, Australia acceded to the First Optional Protocol, which means that Australia recognises that the Human Rights Committee may receive and consider allegations that Australia has violated provisions of the ICCPR. The ICCPR is attached as a schedule to the *Human Rights and Equal Opportunity Act 1986* (Cth). It is also referred to expressly in s 24(1)(b) of the ALRC's enabling Act, the *Australian Law Reform Commission Act 1996* (Cth); see Ch 1 at [1.4] above. See generally Australian Human Rights Information Centre, *A Guide to the Optional Protocol to the International Covenant on Civil and Political Rights*, <www.austlii.edu.au/a/other/ahric/booklet> at 23 December 2003. Note that in *Minister for Immigration and Ethnic Affairs v Teoh* (1995) 183 CLR 273, the High Court held that the ratification of a convention by Australia created a legitimate expectation that decision-makers would take account of that convention.

9 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. Art 6(1) is set out in Appendix 3.

10 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), 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'. It has been stated that an action is a 'suit at law' for the purposes of Art 14 of

national security reasons, it is important that the parameters of the term 'national security' are clearly defined.[11]

7.9 Similarly, Article 10 of the Universal Declaration of Human Rights[12] 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.[13]

7.10 Some Australian legislation expressly provides for open hearings in court. For example, s 17(1) of the *Federal Court of Australia Act 1976* (Cth) provides that:

> Except where, as authorized by this section or another law of the Commonwealth, the jurisdiction of the Court is exercised by a Judge sitting in Chambers, the jurisdiction of the Court shall be exercised in open court.[14]

7.11 Section 54 of the *Supreme Court Act 1933* (ACT) provides that evidence in any matter shall be given in open court, except as otherwise provided by legislation or unless the parties in any suit agree to the contrary. Section 51 of the *Magistrates Court Act 1930* (ACT) provides that hearings are to be held in public although the magistrate presiding can make certain orders including closing the court where he or she is of the opinion that it is 'desirable in the public interest or in the interests of justice to do so'.[15]

---

the ICCPR if the forum where the particular question is adjudicated is one where courts usually exercise control over the proceedings; or the right in question is subject to judicial control or judicial review: See D Weissbrodt, *The Right to a Fair Trial: Articles 8, 10 and 11 of the Universal Declaration of Human Rights* (2001), 125.

11 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), 212. See also discussion in Ch 2.

12 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 the website of Human Rights and Equal Opportunity Commission at <www.hreoc.gov.au/human_rights_dialogue/understanding.html>.

13 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'.

14 *Federal Magistrates Act 1999* (Cth), s 13(2) similarly provides that: 'The jurisdiction of the Federal Magistrates Court must be exercised in open court. However, this rule does not apply where, as authorised by this Act or another law of the Commonwealth, the jurisdiction of the Federal Magistrates Court is exercised by a Federal Magistrate sitting in Chambers.'

15 *Magistrates Court Act 1930* (ACT), s 51(1) and (2). The *Magistrates Court (Civil Jurisdiction) Act 1982* (ACT), s 181(1) and (2) similarly provides that 'except in relation to a matter that may be dealt with in chambers, the hearing of a proceeding before the court shall be in public' although the Magistrate presiding can make certain orders including closing the court where he or she is of the opinion that it is 'desirable in the public interest or in the interests of justice to do so'. See also *Criminal Code* (WA), s 635A(1)

7.12 Some Australian legislation also provides for open hearings in tribunal proceedings. Section 365(1) of the *Migration Act 1958* (Cth) provides that, subject to the section, any oral evidence that the Migration Review Tribunal takes while a person is appearing before it must be taken in public.[16] The *Administrative Decisions Tribunal Act 1997* (NSW) provides that 'if proceedings before the Tribunal are to be determined by holding a hearing, the hearing is to be open to the public.'[17] Hearings before the Federal Police Disciplinary Tribunal generally are to be held in public.[18] Hearings before the Administrative Appeals Tribunal (AAT) are also to be in public unless special circumstances exist—except for proceedings in the Security Appeals Division concerning an application for review of a security assessment, which is to be held in private.[19]

7.13 The *Administrative Appeals Tribunal Act 1975* (Cth) provides that, in considering whether the hearing of a proceeding should be held in private or whether a publication or disclosure to any party of evidence given to, or received by, the AAT should be prohibited or restricted, the AAT:

> shall take as the basis of its consideration the principle that it is desirable that hearings of proceedings before the Tribunal should be held in public and that evidence given before the Tribunal and the contents of documents lodged with the Tribunal or received in evidence by the Tribunal should be made available to the public and to all the parties, but shall pay due regard to any reasons given to the Tribunal why the hearing should be held in private or why publication or disclosure of the evidence or the matter contained in the document should be prohibited or restricted.[20]

7.14 However, legislative provisions that mandate open court hearings except in special circumstances do not of themselves necessarily grant a right of public or media access to court documents. In *The Herald & Weekly Times Ltd v The Magistrates Court of Victoria*, the Victorian Court of Appeal considered that s 125(1) of the *Magistrates' Court Act 1989* (Vic)—which provides for all proceedings in the Magistrates' Court to be conducted in open court except where otherwise provided by legislation or the Rules—did not give a right of access to materials in a hand-up brief at a committal proceeding. A proceeding 'is properly conducted in open court if the public has a right of admission to that court which is reasonably and conveniently exercisable' and an open court does not become closed if a request by a member of the public or the press for access to materials is refused in a committal proceeding.[21]

---

in relation to open criminal proceedings; *Supreme Court Rules* (NT), r 81A.18(1)(a) in relation to open pre-trial hearings; and *Criminal Procedure Amendment (Justices and Local Courts) Act 2001* (NSW), s 191 and Sch 1, s 56 in relation to open summary and committal proceedings respectively.

16 Provisions of the *Migration Act 1958* (Cth) allowing for closed hearings are discussed in Ch 8.

17 *Administrative Decisions Tribunal Act 1997* (NSW), s 75(1). See the exceptions to this rule set out in s 75(2) of the Act.

18 *Complaints (Australian Federal Police) Act 1981* (Cth), s 74(1). The exceptions to this are listed in s 74(2) of the Act, which is set out in the section headed 'Closing tribunals to the public' in Ch 8.

19 See *Administrative Appeals Tribunal Act 1975* (Cth), s 35 and s 39A.

20 Ibid, s 35(3).

21 *The Herald & Weekly Times v The Magistrates' Court of Victoria* [2000] 2 VR 346, [40]. The Court did observe at [42], however, that, if the press is entitled to report upon committal proceedings, it would seem

Principles of open justice

7.15 The principle of open justice is an essential feature of the common law judicial tradition. In *Scott v Scott*, Earl Loreburn declared that 'the inveterate rule is that justice shall be administered in open court' and that the court may be closed only where there was a well-settled exception to the general rule.[22] In *McPherson v McPherson*, the Judicial Committee of the Privy Council reaffirmed the right of the public to be present in courts:

> [P]ublicity is the authentic hallmark of judicial as distinct from administrative procedure …
>
> The actual presence of the public is never of course necessary. Where Courts are held in remote parts of the Province, as they frequently must be, there may be no members of the public to attend. But even so, the Court must be open to any who present themselves for admission. The remoteness of the possibility of any public attendance must never by judicial action be reduced to the certainty that there will be none.[23]

7.16 In *Dickason v Dickason*,[24] the High Court of Australia unanimously applied the principle stated in *Scott v Scott* that there is no inherent power in the court to exclude the public, although that power may be conferred expressly by law.[25] The High Court recognised that 'one of the normal attributes of a court is publicity'.[26] In *Russell v Russell*,[27] 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 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.[28]

7.17 The NSW Court of Appeal has stated that legal proceedings in that State should be heard in public unless the dictates of justice clearly require otherwise.[29] 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

---

desirable that reasonable access to the contents of the hand-up briefs be afforded unless special considerations, such as those contemplated by s 126 of the Act, dictate otherwise. Considerations under the *Magistrates' Court Act 1989* (Vic), s 126 include not endangering the national and international security of Australia, and not prejudicing the administration of justice.

22 *Scott v Scott* [1913] AC 417, 445.

23 *McPherson v McPherson* [1936] AC 177, 200.

24 *Dickason v Dickason* (1913) 17 CLR 50, 51.

25 *Scott v Scott* [1913] AC 417, 473.

26 *Dickason v Dickason* (1913) 17 CLR 50, 51. See also *R v Tait and Bartley* (1979) 24 ALR 473, 487–490.

27 *Russell v Russell* (1976) 134 CLR 495. The legislation in issue was the *Family Law Act 1975* (Cth), s 97(1).

28 Ibid, 520–521.

29 *David Syme & Co Ltd v General Motors-Holden Ltd* [1984] 2 NSWLR 294, 299, 307.

be of constitutional significance'.[30] 'Generally speaking, it is taken for granted that court proceedings are open to the public and may be freely reported.'[31] Chief Justice Spigelman has noted that the exceptions to this principle are few and 'strictly defined'.[32] Kirby P stated in *Raybos Australia Pty Ltd v Jones*:

> The principles which support and justify the open doors of our courts likewise require that what passes in court should be capable of being reported. The entitlement to report to the public at large what is seen and heard in open court is a corollary of the access to the court of those members of the public who choose to attend. …[33]
>
> [T]he principles which support our open courts apply with special force to the open reporting of criminal trials and, by analogy to contempt proceedings … [34]

7.18 The Law Council of Australia's submission to this inquiry adopts 'as a starting point, the cornerstone principle articulated by Jeremy Bentham that publicity is the soul of justice'.[35]

7.19 In the United States, the right to a public trial is expressly guaranteed by the Sixth Amendment to the Constitution:

> 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.

7.20 In Canada, the concept of open courts is embedded in the common law tradition and has found constitutional expression in s 2(b) of the Canadian Charter of Rights and Freedoms,[36] which provides for 'freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication'. The Supreme Court of Canada stated in *Canadian Broadcasting Corp v New Brunswick (Attorney General)* that:

> Openness permits public access to information about the courts, which in turn permits the public to discuss and put forward opinions and criticisms of court practices and proceedings. While the freedom to express ideas and opinions about the operation of the courts is clearly within the ambit of freedom guaranteed by s 2(b), so too is the right of the public to obtain information about the courts in the first place.[37]

---

30 See The Hon JJ Spigelman, 'Seen To Be Done: The Principles of Open Justice—Part 1' (2000) 74 *Australian Law Journal* 290, 292 and generally.

31 See G Nettheim, 'Open Justice and State Secrets' (1986) 10 *Adelaide Law Review* 281, 1.

32 The Hon JJ Spigelman, 'Seen To Be Done: The Principles of Open Justice—Part 1' (2000) 74 *Australian Law Journal* 290, 294 (citations omitted).

33 *Raybos Australia v Jones* (1985) 2 NSWLR 47, 55.

34 Ibid, 58.

35 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

36 *Ruby v Canada (Solicitor General)* (2002) SCC 75, [53].

37 *Canadian Broadcasting Corp v New Brunswick (Attorney General)* [1996] 3 SCR 480, [23] (La Forest J).

7.21 Some other recognised advantages of open justice include increased pressure on witnesses to tell the truth and the possibility that someone hearing the case will know something relevant to the defence.[38] In addition:

> the tendency for publicity to encourage attention of witnesses to the seriousness of the judicial process, … and its promotion of public discussion of judicial matters so that the public 'becomes accustomed to take a deeper interest in their result'.[39]

Access to court documents

7.22 As a practical matter, public access to court proceedings is largely facilitated by mass media reporting of court proceedings, which is necessarily dependent on journalists having access to proceedings, either directly by being permitted to be present while the proceedings transpire or indirectly by being allowed access to relevant documents and transcripts.

7.23 The legislation establishing some Australian courts expressly provides for public access to evidence and other documents produced in relation to proceedings in those courts. However, the legislation and court rules vary from jurisdiction to jurisdiction. Some are more detailed than others in specifying the exact documents to which a non-party may be granted access either with[40] or without the leave of the court.[41] In some cases, there is a presumption that access will be given to documents unless the court otherwise orders;[42] in other cases, the opposite applies.[43] Differences also exist in

---

38 See *R v Shayler* [2003] EWCA Crim 2218, [15], where it is noted that the trial judge did not regard these matters as significant factors in that particular case.

39 *Raybos Australia v Jones* (1985) 2 NSWLR 47, 52, citing J Bentham, *Judicial Evidence* 1825, ch 10.

40 See for example *Supreme Court Rules No 85 1937* (ACT), O 66, r 11(2) which sets out the documents in civil matters that a person who is not party to the proceedings can inspect and copy only if the court's leave has been obtained. See also O 80, r 16(2) and r 16(4). Order 80, r 16(2) sets out the documents in criminal matters that a person who is not party to the proceedings can inspect and copy only if the court's leave has been obtained. These documents include, by way of example, a document that the court has ordered to be kept confidential and an affidavit or a written submission that has not been read out in court. See also *Supreme Court Rules* (NT), r 81A.09(2); and *Supreme Court Act 1935* (SA), s 131(2) which specifies the categories of documents that a member of the public may only inspect or copy with the Court's permission, which includes material that was not taken or received in open court. Section 131(3) provides that if the South Australian Supreme Court grants permission to inspect or copy such material it may impose any condition that it thinks appropriate.

41 For example *Supreme Court Rules* (NT), r 81A.09(1) provides that a person may inspect and copy a document filed in a proceeding that is part of the record of the proceedings of a trial (as defined) while *Supreme Court Act 1935* (SA), s 131(1) sets out the categories of documents that the South Australian Supreme Court must, on application by any member of the public, allow the applicant to inspect or copy. These documents include, by way of example, the transcript of evidence taken by the court, transcript of submissions by counsel, and transcript of the judge's summing up or directions to a jury. *ACT Supreme Court Practice Direction 4: Court Registry—Court Files—Access to by Public—Exceptions*, 26 March 1981 states that subject to a number of specified exceptions 'files in the Supreme Court matters are to be regarded as available for public inspection'. The exceptions include 'affidavits which have not been read in court'; 'any part of affidavits which have been ruled inadmissible in evidence' and 'any proceedings, or parts of proceedings which, by order of a judge, are not to be made public.'

42 See for example, *Supreme Court (General Civil Procedure) Rules 1996* (Vic), r 28.05(1) which provides that any person may inspect and obtain a copy of any document filed in a proceeding, on payment of the proper fee. However, r 28.05(2)(a) and 28.05(2)(b) contain exceptions in relation to confidential documents.

relation to release of transcripts to non-parties. In some cases, it is sufficient for a non-party to make an application for the transcript;[44] in others, the non-party has to show good or sufficient reasons for requesting the transcript.[45]

7.24 For example, the *Federal Court Rules* set out the categories of documents that may be inspected by any person, unless the Court or a judge has ordered that a particular document is confidential. Those documents include, by way of example, originating process, notices of appearance, pleadings, notices of motion or other applications, judgments, orders, written submissions, notices of appeal, and reasons for judgment.[46] The *Federal Court Rules* also provide that certain categories of documents may not be inspected by a person who is not a party to a proceeding without the leave of the Court. These documents are: affidavits (except for specified affidavits in native title proceedings); unsworn statements of evidence filed in accordance with a Court direction; interrogatories and answers to interrogatories; lists of documents given on discovery; admissions; evidence taken on deposition; subpoenas and documents lodged in answer to subpoenas for production of documents; and judgments, orders or other documents that the Court has ordered are confidential.[47] Further, the Court's leave must be obtained for either a party or a non-party to proceedings to inspect a transcript of the proceedings or a document 'filed in support of an application for an order that a document, evidence or thing be privileged from production'.[48]

7.25 Some lower courts also have provisions in their legislation governing media access to court documents. Section 314 in Schedule 1 of the *Criminal Procedure Amendment (Justices and Local Courts) Act (2001)* (NSW), which came into force in July 2003, provides that:

> (1) A media representative is entitled to inspect documents set out in subsection (2) relating to criminal proceedings if an application to do so is made to the registrar not later than 2 working days after the proceedings are finally disposed of and the inspection is for the purpose of compiling a fair report of the proceedings for publication.
>
> (2) The documents are copies of the indictment, court attendance notice or other document commencing the proceedings, witnesses' statements tendered as

---

43 See for example, *Supreme Court (Criminal Procedure) Rules 1998* (Vic), r 1.11(4) which provides that a document filed in proceedings to which the Rules relate is *not* open for inspection unless the Court so directs. See also *Supreme Court Rules 1970* (NSW), Part 65, r 7. Part 65, r 7(1) provides that a 'person may not search in a registry for or inspect any document or thing in any proceedings except with the leave of the Court.' Subject to certain specified exceptions, Part 65, r 7(1) does not apply to a party to the proceedings: see Part 65, r 7(2), (2A) and (3).

44 See *Supreme Court Act 1935* (SA), s 131(1)(a),(c), (d) and (e).

45 See for example, *Criminal Procedure Rules 2000* (WA), r 76(1)–(3). See also *Supreme Court Act 1933* (ACT), s 74A(5) and (6). The *Magistrates Court Act 1930* (ACT), s 255C(2) also provides that a registrar shall not provide a non-party to a proceeding to which a transcript relates with a copy of the transcript unless the registrar or a magistrate is satisfied that the non-party has good reason for applying for the transcript.

46 See *Federal Court Rules 1979* , O 46, r 6(1) and (2).

47 See Ibid, O 46, r 6(3).

48 See Ibid, O 46, r 6(5).

> evidence, brief of evidence, police fact sheet (in the case of a guilty plea), transcripts of evidence and any record of a conviction or an order. …
>
> (4) The registrar must not make documents available for inspection if:
>
> (a) the proceedings are subject to an order prohibiting their publication, a suppression order or are held in closed court, or
>
> (b) the documents are prohibited from being published or disclosed by or under any other Act or law.

7.26 The NSW Government stated that the legal amendment gave the media for the first time a statutory right of access to court documents.[49] The NSW Government reportedly urged all court registrars to permit media access to court documents, following expressions of concern that the new legislation would threaten press freedom.[50] Opponents of the new law argued that it would prevent access to once freely available court documents until a case was finished.[51] The Opposition legal spokesman, Mr Andrew Tink, said that the changes meant that bail applications, in particular, 'will effectively become secret hearings.'[52] Mr Bruce Wolpe, the manager of corporate affairs for the Fairfax media organisation, said that the law challenged 'a free press and open justice.'[53] However, a consultation with media representatives suggested that, following education about the interpretation of s 314, it now appeared to be working well.[54]

7.27 A series of United States cases has developed a set of rules relating to the right of the public to inspect and copy court records, in which it has been said that it is for the court to devise a plan for the release of the materials to which access has been requested. For example, in *United States v Mitchell*, a television station sought access to parts of President Nixon's White House tapes that had been played to the jury in a criminal trial. Access was allowed, the court holding that the common law right to inspect and copy judicial records extends to exhibits and that:

> the parties and the court will have to attempt to develop a plan for release of the tapes … Distribution should be prompt, and on equal basis to all persons desiring copies. The court cannot be expected to assume the cost of distribution, nor should the court's time or personnel be unduly imposed upon.[55]

---

49 S Gibbs, 'Court Rules under Fire from Media', *The Sydney Morning Herald*, 8 July 2003, 5.

50 'Fears over Court Access', *The Australian*, 8 July 2003, 8. The NSW Attorney-General, Bob Debus, invited media organisations to make submissions about their concerns.

51 S Gibbs, 'Court Rules under Fire from Media', *The Sydney Morning Herald*, 8 July 2003, 5.

52 Ibid.

53 Ibid.

54 Commercial Television Australia, *Consultation*, Sydney, 11 September 2003.

55 *United States v Mitchell* 551 F 2d 1252 (1976), 1265. This was reversed on other grounds in *sub nom Nixon v Warner Communications Inc* 435 US 589 (1978), 598–599, where the US Supreme Court held that the common law right of access is not absolute and that the decision whether to allow access should be left to the sound discretion of the trial court.

7.28 In *United States v Myers*, television networks sought to copy and televise video tapes admitted into evidence in a criminal trial. The court considered that, once material had become evidence at a public session of the trial, access should be permitted for inspection and copying. The court stated that as long as there was no significant risk of damaging the integrity of the evidence or interfering with the orderly conduct of the trial, only the most compelling circumstances could prevent contemporaneous public access to it.[56]

7.29 In 2003, *The Vancouver Sun* sought access to material filed in, or arising from, in-camera proceedings concerning the interpretation and application of the new s 83.28 of the Canadian *Criminal Code*,[57] which provides for investigative hearings in relation to terrorism offences, and for a declaration that neither the proceedings to date nor any future proceedings should be heard in camera. *The Vancouver Sun* sought access by a two-stage process.

> At the proposed first stage counsel for the applicant would file an undertaking for confidentiality, and would have an opportunity to view the material in question under specified terms, along with one or two members of the applicant's editorial board who would be subject to the same restrictive terms. This is proposed as a means of enabling the applicant to know enough about the proceedings to determine whether or not to pursue the application to the second stage of seeking access and publication in the ordinary fashion and without restrictive terms. Similar two staged approaches were taken in the cases of *Clark v The Queen* (20 August 1999), Vancouver, BL0146 (BCSC), *Pacific Press Ltd v Canada (Minister of Employment and Immigration)*, [1990] 1 FC 419 (CA) and *R v A*, [1990] 1 SCR 992.[58]

7.30 In rejecting *The Vancouver Sun's* application, Holmes J of the Supreme Court of British Columbia referred to previous decisions of the Supreme Court of Canada in relation to publication bans. In *CBC v Dagenais*, the Supreme Court concluded that a publication ban should only be ordered when:

> (a) such a ban is necessary in order to prevent a real and substantial risk to the fairness of the trial, because reasonably alternative measures will not prevent the risk; and
>
> (b) the salutary effects of the publication ban outweigh the deleterious effects to the free expression of those affected by the ban.[59]

---

56 *United States v Myers* 635 F 2d 945 (1980) as discussed in *The Herald & Weekly Times v The Magistrates' Court of Victoria* [2000] 2 VR 346, [22].

57 *Criminal Code* [RS 1985, c C–46] (Canada), s 83.28 enables a peace officer to make an ex parte application to a judge for an order for the gathering of information. The judge must be satisfied that the Attorney General has consented to the application, and that there are reasonable grounds to believe that a terrorism offence has been committed or is about to be committed, and that the person named in the order to attend for an examination has relevant information.

58 *In the Matter of an Application under s 83.28 of the Criminal Code and The Vancouver Sun* (2003) BCSC 1330, [2]. This case is also discussed at [7.101] below.

59 *CBC v Dagenais* [1994] 3 SCR 835, 878.

7.31 In *R v Mentuck*, the *Dagenais* test was restated to incorporate a consideration of interests in addition to fair trial rights, including the proper administration of justice and the integrity of investigations. The Supreme Court stated that a publication ban should only be ordered where:

> (a) such an order is necessary in order to prevent a serious risk to the proper administration of justice because reasonably alternative measures will not prevent the risk; and
>
> (b) the salutary effects of the publication ban outweigh the deleterious effects on the rights and interests of the parties and the public, including the effects on the right to free expression, the right of the accused to a fair and public trial, and the efficacy of the administration of justice.[60]

7.32 Holmes J stated that, although the Supreme Court of Canada reformulated the *Dagenais* test:

> to accommodate the consideration of the public interest in effective police investigations, it did so in the context of a trial or trial proceedings where the public interest in open access is incontrovertibly high.[61]

7.33 Holmes J distinguished the proceedings under s 83.28 of the Canadian *Criminal Code* on the basis that it related to the investigative process, and that features of the investigative process rendered many investigative procedures 'inherently inappropriate for public scrutiny at the stage before they are completed.'[62] One example of an investigative procedure that was inherently inconsistent with public access was proceedings relating to the issue of search warrants.[63] Her Honour noted *The Vancouver Sun's* argument that s 83.28 does not expressly provide for the proceedings to be heard in camera, but the same could be said of the provisions relating to the issue of search warrants, and she drew no inference from Parliament's failure to expressly provide for in-camera hearings for proceedings arising under s 83.28. *The Vancouver Sun* has sought leave to appeal the decision to the Supreme Court of Canada.[64]

Procedural protections in criminal proceedings

7.34 Certain procedural protections provided for in international instruments apply exclusively to criminal proceedings.[65] Article 14(3) of the International Covenant on

---

60 *R v Mentuck* [2001] 3 SCR 442, [32]. The Supreme Court stated that the risk to the administration of justice relied upon to support a publication ban had to be 'real and substantial', 'well grounded in the evidence', and that there had to be a 'serious danger sought to be avoided … not a substantial benefit or advantage to the administration of justice sought to be obtained': *R v Mentuck* [2001] 3 SCR 442, [34].

61 *In the Matter of an Application under s 83.28 of the Criminal Code and The Vancouver Sun* (2003) BCSC 1330, [15].

62 Ibid, [26]. Holmes J noted that different consideration could apply after the investigative procedure was over.

63 See Ibid, [19]–[22].

64 An application for leave to appeal was filed on 1 August 2003.

65 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. These

Civil and Political Rights (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;[66]

(b) To have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;[67]

(c) To be tried without undue delay;

(d) To be tried in his presence,[68] 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;[69]

(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.[70]

---

articles are set out in full in Appendix 3. Note also that the *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 under that Act.

66 The Human Rights Committee has stated that the right to be informed of the charge 'promptly' requires 'that information is given in the manner described as soon as the charge is first made by a competent authority. In the opinion of the Committee this right must arise when in the course of an investigation a court or an authority of the prosecution decides to take procedural steps against a person suspected of a crime or publicly names him as such': Office of the High Commissioner for Human Rights, *Equality Before the Courts and the Right to a Fair and Public Hearing by an Independent Court Established by Law (Art 14): 13/04/84. CCPR General Comment 13*, <www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+13.En?OpenDocument/>, [8].

67 The issue of choice of counsel is addressed in Ch 6.

68 The right to be tried in one's presence is discussed further at [7.55].

69 'The right to be defended by counsel includes the right to notification of the right to counsel, the right of access to and confidential communications with counsel and the right to assistance by counsel of choice or by qualified appointed counsel.' Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, 20.3. 'The right to be represented by a lawyer of one's choice may be restricted if the lawyer is not acting within the bounds of professional ethics, is the subject of criminal proceedings or refuses to follow court procedure.' Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, 20.3.2. The provision of legal aid services is discussed in Ch 6.

70 Article 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 limited 'to the extent strictly required by the exigencies of the situation', (that is, proportionate), are not inconsistent with their other obligations under international law and are not discriminatory. Article 4 sets out articles of the convention that are not subject to derogation. The full text of Art 4 is set out in Appendix 3. State Parties may not invoke Art 4 as justification for 'deviating from fundamental principles of fair trial, including the presumption of innocence'. 'As certain elements of the right to a fair trial are explicitly guaranteed under international humanitarian law during armed conflict, the [Human Rights] Committee finds no justification for derogation from these guarantees during other emergency

7.35 Adherence to these minimum guarantees does not in all cases and circumstances ensure that a trial has been fair. Amnesty International asserts that 'the right to a fair trial is broader than the sum of the individual guarantees, and depends on the entire conduct of the trial.'[71] Further, 'the broader right to a fair trial applies as soon as the government suspects that an individual has committed an offence and continues through charge, arrest, preliminary hearings, trial, appeal, other post-conviction review, and punishment.'[72]

7.36 Article 14 of the ICCPR applies to all trials, in all courts, whether ordinary or special. The Human Rights Committee of the United Nations has stated that, while the ICCPR does not prohibit trials of civilians in special or military courts, 'the trying of civilians by such courts should be very exceptional and take place under conditions which genuinely afford the full guarantees stipulated in Article 14'.[73]

7.37 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.

7.38 Amnesty International has expressed the view that:

> All criminal and administrative proceedings should be conducted in accordance with internationally recognized fair trial rights.
>
> Secret evidence and anonymous witnesses should not be used in criminal trials, proceedings to determine refugee status, or proceedings to determine whether a person should be detained on the grounds that they are a threat to national security.[74]

7.39 In *Van Mechelen v The Netherlands*, the European Court of Human Rights (ECHR) stated that the use of statements made by anonymous witnesses to found a

---

situations. The Committee is of the opinion that the principles of legality and the rule of law require that fundamental requirements of fair trial must be respected during a state of emergency. Only a court of law may try and convict a person for a criminal offence.' See Human Rights Committee, *General Comment 29, States of Emergency (Article 4), UN Doc CCPR/C21/Rev Add 11*, [11], [16]. Further, the fact that Art 14 is not expressly mentioned in Art 4 as not being subject to non-derogation does not mean that it may be subjected to derogations at will, even where a threat to the life of the nation exists: see Human Rights Committee, *General Comment 29, States of Emergency (Article 4), UN Doc CCPR/C21/Rev Add 11*, [6]. 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'.

71 Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, 13.1 [citations omitted].

72 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003.

73 Office of the High Commissioner for Human Rights, *Equality Before the Courts and the Right to a Fair and Public Hearing by an Independent Court Established by Law (Art 14): 13/04/84. CCPR General Comment 13*, <www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+13.En?OpenDocument/> [4].

74 Amnesty International, *Rights at Risk: Amnesty International's Concerns regarding Security Legislation and Law Enforcement Measures* (2002), 37.

conviction was not under all circumstances incompatible with the European Convention on Human Rights—for example where the life, liberty or security of a witness might be at stake.[75]

> [A]ll the evidence must normally be produced at a public hearing, in the presence of the accused, with a view to adversarial argument. There are exceptions to this principle, but they must not infringe the rights of the defence; as a general rule paragraphs 1 and 3(d) of Article 6[76] … require that the defendant be given an adequate and proper opportunity to challenge and question a witness against him, either when he makes his statements or at a later stage …
>
> [T]he use of statements made by anonymous witnesses to found a conviction is not under all circumstances incompatible with the Convention …
>
> However, if the anonymity of prosecution witnesses is maintained, the defence will be faced with difficulties which criminal proceedings should not normally involve. Accordingly, the Court has recognised that in such cases Article 6 para 1 taken together with Article 6 para 3(d) of the Convention … requires that the handicaps under which the defence labours be sufficiently counterbalanced by the procedures followed by the judicial authorities …
>
> Finally, it should be recalled that a conviction should not be based either solely or to a decisive extent on anonymous statements …
>
> Having regard to the place that the right to a fair administration of justice holds in a democratic society, any measures restricting the rights of the defence should be strictly necessary. If a less restrictive measure can suffice then that measure should be applied.[77]

7.40 The applicants in *Van Mechelen* complained that their convictions were essentially based on the evidence of police officers whose identities were not made known to them, and whose evidence was not given in public or in their presence. A judge ascertained the identity of the police officers and took statements from them. The judge produced a report in which he expressed his opinion about the reliability and credibility of the witnesses and found their reasons for wanting to remain anonymous to be sufficient.[78] However, the ECHR found that these measures could not be considered 'a proper substitute for the possibility of the defence to question the witnesses in their presence and make their own judgment as to their demeanour and reliability.'[79] The proceedings were held to be unfair, the ECHR stating:

> In the present case, the police officers in question were in a separate room with the investigating judge, from which the accused and even their counsel were excluded.

---

75 See *Van Mechelen v The Netherlands* (1997) III Eur Court HR 691, [52]–[53], applying *Doorson v The Netherlands* (1997) II Eur Court HR 446, 470.

76 Art 6(1) of the European Convention on Human Rights is in similar terms to Art 14(1) of the ICCPR, and Art 6(3)(d) of the European Convention on Human Rights is similar to Art 14(3)(e) of the ICCPR. The text of both Articles is set out in Appendix 3.

77 *Van Mechelen v The Netherlands* (1997) III Eur Court HR 691, [51]–[52], [54]–[55], [58] (citations omitted).

78 Ibid, [48].

79 Ibid, [62].

> All communication was via a sound link. The defence was thus not only unaware of the identity of the police witnesses but also prevented from observing their demeanour under direct questioning, and thus from testing their reliability …
>
> It has not been explained to the Court's satisfaction why it was necessary to resort to such extreme limitations on the right of the accused to have the evidence against them given in their presence, or why less far-reaching measures were not considered.[80]

7.41 In determining that the proceedings were unfair, the ECHR had regard to the fact that the anonymous witness statements were the *only* evidence relied upon by the Court of Appeal which provided positive identification of the applicants as the perpetrators of the crime.[81]

7.42 The right to a fair trial is constitutionally 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 entrenched in the Commonwealth Constitution by Ch III's implicit requirement that judicial power be exercised in accordance with the judicial process.[82] Otherwise the 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.[83]

7.43 Deane J similarly stated that:

> The fundamental prescript of the common law of this country is that no person shall be convicted of a crime except after a fair trial according to law. In so far as the exercise of the judicial power of the Commonwealth is concerned, that principle is entrenched by the Constitution's requirement of the observance of judicial process and

80 Ibid, [59]–[60].
81 Ibid, [63].
82 See the discussion on Chapter III issues in Ch 9.
83 *Dietrich v The Queen* (1992) 177 CLR 292, 362–364.

> fairness that is implicit in the vesting of the judicial power of the Commonwealth exclusively in the courts which Ch III of the Constitution designates.[84]

7.44 In *Polyukhovich v The Commonwealth*, Gaudron J described the inherent power to stay proceedings as 'an essential attribute of a superior court' that 'exists for the purpose of ensuring that proceedings serve the ends of justice and are not themselves productive of or an instrument of injustice'.[85] Her Honour stated that, in order to interfere with such an 'important and essential power' Parliament would have to use 'unmistakable language' but warned that if it did so:

> A question might arise, at least in circumstances which would call for the exercise of that power, whether its curtailment or abrogation transformed the power purportedly vested in the court into something other than judicial power and, thus, brought the provision into conflict with Ch III.[86]

7.45 In Canada, the power of a judge presiding at a criminal trial to make any order that he or she considers appropriate in the circumstances to protect the right of the accused to a fair trial, is expressly provided for in the *Canada Evidence Act.*[87] Possible orders include:

> (a) an order dismissing specified counts of the indictment or information, or permitting the indictment or information to proceed only in respect of a lesser or included offence;
>
> (b) an order effecting a stay of the proceedings; and
>
> (c) an order finding against any party on any issue relating to information the disclosure of which is prohibited.[88]

7.46 It is important to note that, where an objection has been made by a Canadian Government Minister or other official to the disclosure of information on the grounds of a specified public interest, the court's power to make these orders protecting the accused's right to a fair trial is subject to compliance with the terms of any order made by the court in determining that objection.[89] In the case of information which, if dis-

---

84 Ibid, 326. One commentator has stated: 'It would seem to follow then that Deane J and Gaudron J believe that it would be contrary to Chapter III of the [*Australian Constitution*] for Parliament to abrogate or, at least in certain circumstances, curtail the inherent power of a court exercising federal jurisdiction to stay proceedings to prevent an unfair criminal trial.' See F Wheeler, 'The Doctrine of Separation of Powers and Constitutionally Entrenched Due Process in Australia' (1997) 23 *Monash University Law Review* 248, 266. Note that Toohey J stated in *Dietrich v The Queen* (1992) 177 CLR 292, 353 that the 'concept of a fair trial is one that is impossible, in advance, to formulate exhaustively or even comprehensively. Only a body of judicial decisions gives content to the concept.'

85 *Polyukhovich v The Commonwealth* (1991) 172 CLR 501, 703.

86 Ibid, 703. This case concerned the constitutional validity of a federal provision creating a retrospective criminal offence.

87 *Canada Evidence Act* [RS 1985, c C–5] , s 37.3(1), and 38.14(1).

88 Ibid, s 37.3(2) and s 38.14(2).

89 The orders that the court can make in determining an objection to disclosure are orders to disclose the information, to disclose the information subject to any conditions that the court considers appropriate or to prohibit disclosure. See Ibid, s 37(4.1)–(6).

closed, would be injurious to international relations or national defence or national security, the court's ability to make an order protecting the accused's right to a fair trial is also subject to compliance with any order made in relation to those proceedings concerning the disclosure of such information, or any judgment made on appeal or review of that order, or any certificate issued by the Attorney General prohibiting the disclosure of the information.[90]

7.47 The ACT Government has introduced a Bill of Rights in the form of a Human Rights Act based on the rights set out in the ICCPR. One of the rights that will be protected by the legislation is the right to a fair trial based on Article 14 of the ICCPR. The legislation will require courts and tribunals to interpret laws to be compatible with the Human Rights Act as far as possible but will not give a direct right of court action to enforce those rights.[91]

The right to trial by jury

7.48 The right to a trial by jury for indictable offences against Commonwealth law is preserved by s 80 of the *Australian Constitution*.[92] 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.[93] Deane J stated that s 80 'is not framed in terms of mere privilege. Its words are mandatory. Its command is unqualified.'[94] He said that s 80 was an 'important constitutional guarantee against the arbitrary determination of guilt or innocence' that operated for 'the benefit of the community as a whole as well as for the benefit of the particular accused'.[95] Dawson J stated that '[n]o doubt the section confers a benefit on every person charged on indictment under a

90 See Ibid, s 38.14(1). The orders that the court can make in relation to the disclosure of national security information are orders authorising the disclosure, to disclose the information subject to any conditions that the court considers appropriate or to prohibit disclosure. See *Canada Evidence Act* [RS 1985, c C–5], s 38.06(1)–(3). The orders that the court can make concerning disclosure and the certificates that can be issued by the Attorney General of Canada under the Act are discussed in Ch 8.

91 See J Stanhope MLA (Chief Minister and Attorney-General), *Bill of Rights for the ACT*, Media Release 352/03, 22 October 2003 and Government of the Australian Capital Territory, *Government Response to the Report of the ACT Bill of Rights Consultative Committee*. The ACT Government has proposed that the legislation not come into force until 1 July 2004.

92 Section 80 is set out in full in Appendix 3. Defendants can elect to be tried by judge alone when charged with a state indictable offence. New South Wales, the Australian Capital Territory, South Australia and Western Australia allow an accused person in criminal proceedings to elect trial by judge alone. See *Criminal Procedure Act 1986* (NSW), s 132; *Supreme Court Act 1933* (ACT), s 68B; *Juries Act 1927* (SA), s 7; and *Criminal Code* (WA), s 651A–651C. In New South Wales, the Australian Capital Territory and South Australia the trial judge must be satisfied that the accused has received legal advice in relation to the decision to proceed by judge alone. In New South Wales, such an election can only be made with the consent of the Director of Public Prosecutions.

93 *Brown v R* (1986) 160 CLR 171.

94 Ibid, 201. But in the US, Frankfurter J said that this view about the non-waiver of jury trials was to 'imprison a man in his privileges and call it the Constitution': *Adams v US* 317 US 269, 280.

95 Ibid, 201.

Commonwealth law, but its benefits extend beyond the individual and its guarantee is more than personal.'[96]

7.49 One commentator has noted that:

> In also denying the possibility that a trial by jury may be waived, Dawson J placed emphasis upon the constitutional context. Section 80 is located in Ch III of the *Constitution*: an unlikely repository, in his Honour's view, for a provision by way of a guarantee 'with a private rather than a public significance'.[97]

7.50 In *Cheatle v The Queen*, the High Court unanimously held that s 80 of the *Australian Constitution* prevented majority jury verdicts in Commonwealth trials, since unanimity was an essential element of trial by jury.[98] The High Court also noted that a jury must be 'representative of the wider community'.[99] One commentator has stated that *Cheatle* and *Katsuno v The Queen*[100] make it clear that random selection and impartiality are fundamental features of a trial by jury for the purposes of s 80.[101]

> Contemporary jury rules and practices will be incompatible with s 80 of the *Constitution* if they are incompatible with the functional attributes of a trial by jury. As to what those attributes are, their Honours all seem to gravitate towards representativeness, impartiality, randomness, measured group deliberation, and the efficient administration of justice.[102]

7.51 It is Parliament that determines the circumstances in which an offence against the law of the Commonwealth will be tried on indictment.[103] In *R v Archdall and Roskruge; Ex Parte Corrigan and Brown*, the offence in question was punishable either on indictment or on summary conviction. The prosecution argued that the offence could not be 'declared by Parliament to be other than indictable' as the offence

---

96 Ibid, 209. However, Gibbs CJ (at 179) expressed the view that s 80 was 'inserted for the benefit of persons accused of offences against the law of the Commonwealth and not for any wider public interest.'

97 J Stellios, 'Section 80 of the Constitution—"A Bulwark of Liberty?"' (Paper presented at The Australian Constitution in Troubled Times conference, Canberra, 7–9 November 2003), 105 and see *Brown v R* (1986) 160 CLR 171, 208. Stellios argues (at 120) that s 80 itself is not 'a bulwark of liberty'. 'It is a fundamental structural or institutional provision that facilitates the exercise of Commonwealth judicial power in a federation. It may be fully accepted that *a jury trial* is '*a* bulwark of liberty', however, in our constitutional system of government, it remains a common law right, the preservation of which rests with the system of representative and responsible government created by the *Constitution*.'

98 *Cheatle v The Queen* (1993) 177 CLR 541. See *Fittock v The Queen* [2003] HCA 19, [8], [9], [21] and [39] which held that the reserve juror provisions in the *Juries Act 1962* (NT) did not conflict with what was required of a fair trial 'by jury' within the meaning of s 80 of the *Constitution* and 'that it was impossible to read into s 80 an implication that there cannot be a trial by jury where reserve jurors are selected in addition to 12 jurors'. See also *Ng v R* [2003] HCA 20 [12] and [64]–[65], where it was held that there was no prejudice to the principle of unanimity of a jury where there was a discharge because of death or incapacity or the excusing of additional jurors who were balloted out under the procedures set out in *Juries Act 1967* (Vic), s 48A.

99 *Cheatle v The Queen* (1993) 177 CLR 541, 560.

100 *Katsuno v The Queen* (1999) 199 CLR 40.

101 J Stellios, 'Section 80 of the Constitution—"A Bulwark of Liberty?"' (Paper presented at The Australian Constitution in Troubled Times conference, Canberra, 7–9 November 2003), 89.

102 Ibid, 93. These are matters that may be relevant to any proposed security clearances of jurors: see Ch 6. Stellios argues (at 89) that, as a general proposition, jury vetting is not incompatible with s 80.

103 Ibid, 77.

was an indictable one at federation.[104] The High Court rejected the argument, stating that the 'suggestion that the Parliament, by reason of [section] 80 of the *Constitution* could not validly make the offence punishable summarily has no foundation and its rejection needs no exposition.'[105]

7.52 In *Kingswell v The Queen*, the High Court said:

> It has been held that s 80 does not mean that the trial of all serious offences shall be by jury; the section applies if there is a trial on indictment, but leaves it to the Parliament to determine whether any particular offence shall be tried on indictment or summarily. This result has been criticized, but the Court has consistently refused to reopen the question and the construction of the section should be regarded as settled …[106]

7.53 As a consequence of s 80, in cases alleging the unauthorised disclosure of classified or security sensitive information, whenever the content, quality or effect of that information is an issue in the case, the information must almost certainly be disclosed to the jury as the offences are currently structured—especially where it is an element of either the offence itself or a defence.

7.54 This issue arose in the prosecution of Simon Lappas, a former Defence Intelligence Organisation analyst.[107] Two of the documents upon which the prosecution sought to rely emanated from a foreign power which declined to allow the contents of the documents to be shown to a non-security cleared jury. However, given that the charge involved an element of intention to cause detriment to the safety or defence of the Commonwealth and to assist a foreign power, in the absence of an admission from the defence as to the effect of those documents and Lappas's intention in that regard, it was impossible to proceed to try those offences without showing the documents to the jury.[108] Accordingly, the prosecution proceeded with lesser 'disciplinary' charges under s 78(3) of the *Crimes Act 1914* (Cth) of having removed from his workplace and given to an unauthorised person a document which he was not entitled to deal with in

---

104 *R v Archdall and Roskruge; Ex parte Corrigan and Brown* (1928) 41 CLR 128, 133.

105 Ibid, 135. Higgins J in the same case also rejected the argument, stating that 'if there be an indictment, there must be a jury; but there is nothing to compel procedure by indictment'.

106 *Kingswell v The Queen* (1985) 159 CLR 264, 276–277 (Gibbs CJ, Wilson and Dawson JJ). Deane J dissented on this point (at 319). He considered that there would be a trial on indictment for the purposes of s 80 where the accused, if found guilty, would stand convicted of a 'serious offence' which was one that could not be 'appropriately dealt with summarily by justices or magistrates in that conviction will expose the accused to grave punishment.' See also *R v The Federal Court of Bankruptcy; Ex parte Lowenstein* (1938) 59 CLR 556, 570, where Latham CJ (with Rich J agreeing) expressed the view that *R v Archdall and Roskruge; Ex parte Corrigan and Brown* (1928) 41 CLR 128 was authority for stating that 'sec 80 did not prevent the Commonwealth Parliament from determining whether any particular offence should be prosecuted on indictment or summarily'. Dixon and Evatt JJ dissented, expressing the view that to allow Parliament to determine for itself what offences should be tried on indictment would 'mock' the constitutional provision: see *R v The Federal Court of Bankruptcy; Ex parte Lowenstein* (1938) 59 CLR 556, 581–582.

107 The prosecution of Simon Lappas and the offences with which he was charged are discussed further at [7.76]–[7.79] and in Appendix 4.

108 Advisory Committee member, *Consultation*, Melbourne, 29 August 2003.

that way. Lappas pleaded guilty to these charges. Whether he could have insisted upon the contents of the document being admitted into evidence, and consequently being put before the jury, was never tested. On one view, he could probably not have so insisted.[109]

The right to be present at one's trial

7.55 As stated above, an accused has a right to be tried in his or her presence, and to examine or have examined the witnesses against him or her.[110] However, the right to be present is not unqualified. It has been said that:

> The right of an accused to be present at trial may be temporarily restricted if the accused disrupts the court proceedings to such an extent that the court deems it impractical for the trial to continue in his or her presence. The Human Rights Committee has stated that it may also be relinquished if the accused fails to appear in court for trial after having been duly notified of the proceedings.[111]

7.56 In *R v Abrahams*, Williams J in the Supreme Court of Victoria stated:

> [I]n all criminal trials the prisoner has a right, as long as he conducts himself decently, to be present, and ought to be present, whether he is represented by counsel or not. He may waive this right if he so pleases, and may do this even in a case where he is not represented by counsel. But then a further and most important principle comes in, and that is, that the presiding Judge has a discretion in either case to proceed or not to proceed with the trial in the accused's absence. In the case where the prisoner is not represented by counsel, and waives his right to be present, the Judge would in all probability, having regard to the principle just stated, that a prisoner ought to be present, exercise his discretion by not proceeding with the trial in the absence of the accused, and if in such a case the prisoner's desire not to be present were occasioned by indisposition, the Judge, if such indisposition were likely to be prolonged, would probably exercise his discretion by discharging the jury.[112]

7.57 Some Australian and overseas legislation expressly 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.[113]

---

109 Advisory Committee member, *Correspondence*, 18 September 2003.

110 See [7.34] above.

111 Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, 21.1. 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'.

112 *R v Abrahams* (1895) 21 VLR 343, 346.

113 However, *Criminal Procedure Amendment (Justices and Local Courts) Act 2001* (NSW), s 72(1) allows the magistrate to excuse the accused from attending during the taking of prosecution evidence if satisfied

7.58 The *Criminal Code* (WA) also provides for the presence of the accused:

> The trial must take place in the presence of the accused person, unless he so conducts himself as to render the continuance of the proceedings in his presence impracticable, in which case the court may order him to be removed, and may direct the trial to proceed in his absence.
>
> Provided that the court may, in any case, if it thinks fit, permit a person charged with a misdemeanour to be absent during the whole or any part of the trial on such conditions as it thinks fit.[114]

7.59 However, some statutes establishing Australian courts, and some court rules, do not expressly provide for the presence of the accused in criminal proceedings—although in some cases they appear to imply it. For example, the *Supreme Court Act 1933* (ACT) provides that:

> A party in a cause[115] or matter may appear before the court either personally or by a legal practitioner having the right to practise in the court.[116]

7.60 The Act also provides that:

> When there are several defendants in any cause pending in the court, if any defendant is not served with process and does not voluntarily appear, the court may nevertheless entertain the cause and proceed to hear and determine it between the parties who are properly before the court.[117]
>
> The judgment referred to in subsection (1) in a cause does not prejudice a defendant in the cause who is not served with process and does not voluntarily submit to the jurisdiction of the court.[118]

7.61 The *Supreme Court Rules 1970* (NSW) provide that:

> (1) If, when a trial is called on, any party is absent, the Court may, on terms:

---

that the accused will have legal representation while the evidence is being taken or is satisfied that the evidence is not applicable to the accused. Section 73 of the Act allows the evidence to be taken in the absence of an accused who has not been excused from attending if no good reason is presented for the accused's absence and a copy of any relevant material has been served on the accused and the accused has been notified of the time set by the magistrate for taking prosecution evidence.

114 *Criminal Code* (WA), s 635. This section also provides that it does not prevent a court from taking evidence from an accused by audio or video link under the *Evidence Act 1906* (WA). See also the *Criminal Code* [RS 1985, c C–46] (Canada), s 650, which provides that an accused, other than a corporation, is to be present during the whole of his or her trial. Provision is made for the accused to appear by counsel or by closed-circuit television where the court orders and the prosecutor and accused agree. The court may also cause the accused to be removed from court where he or she interrupts the proceedings so that to continue in his or her presence would not be feasible.

115 'Cause includes any suit, and also includes criminal proceedings': *Supreme Court Act 1933* (ACT), Dictionary.

116 Ibid, s 56.

117 Ibid, s 58(1).

118 Ibid, s 58(2). The *Supreme Court Rules No 85 1937* (ACT), O 38, r 10 provides, in relation to the civil jurisdiction of the Court, that: 'If, when a trial is called on, the plaintiff appears, and the defendant does not appear, then the plaintiff may prove his or her claim, so far as the burden of proof lies on him or her'.

(a) order that the trial be not had unless the proceedings are again set down for trial, or unless such other steps are taken as the Court may direct,

(b) proceed with the trial generally or so far as concerns any claim for relief in the proceedings, or

(c) adjourn the trial.

(2) Where the Court proceeds with a trial in the absence of a party, and at or at the conclusion of the trial a verdict is given or a finding or assessment is made, the Court, on motion by that party, may, on terms, set aside or vary the verdict, finding or assessment, and may give directions for the further conduct of the proceedings.

(3) Subrule (2) does not enable the Court to vary the verdict, finding or assessment of a jury at a trial except with the consent of each interested party present at the trial.[119]

7.62 Some court rules make provision in relation to the absence of a party at the hearing of an appeal.[120]

The right to 'equality of arms'

7.63 A necessary characteristic of a fair hearing is the adherence to the principle of 'equality of arms' between the parties in a case, which aims to ensure that parties are in a procedurally equal position. In criminal trials, the principle is a guarantee of the right to defend oneself and includes the rights to legal counsel, to call and examine witnesses, to be present at one's trial, and to disclosure by the prosecution of all material information.[121]

7.64 In *Rowe and Davis v The United Kingdom*, the European Court of Human Rights (ECHR) stated:

---

119 *Supreme Court Rules 1970* (NSW), Part 34, r 5. Part 34, r 2 provides that Part 34 applies to proceedings commenced by statement of claim and, subject to Part 34, r 3 to 'proceedings commenced by summons to such extent and with such modifications as the Court may direct'. Part 5, r 9, which applies in relation to proceedings commenced by summons, provides that the court may proceed in the absence of a plaintiff where he or she has had due notice of the hearing, and in the absence of a defendant where he or she is either in default of appearance or has had due notice of the hearing. See also *Supreme Court Rules 1970* (NSW), Part 75, r 11A which applies to proceedings in the Court under Part 5 of Chapter 4 of the *Criminal Procedure Act 1986* (NSW). That rule allows in certain circumstances a trial to proceed in the absence of a defendant where he or she has been given notice of the hearing.

120 For example, *Supreme Court (Criminal Procedure) Rules 1998* (Vic), r 2.28.1(1) provides that 'The appellant is entitled to be present on the hearing of an appeal or an application to the Court of Appeal unless the Court of Appeal or a Judge of Appeal directs otherwise.' Rule 2.28.1(2) provides that 'If the appellant does not attend court on the hearing, the appeal or the application may be heard and determined in the appellant's absence.' The *Supreme Court Rules No 85 1937* (ACT), O 86, r 47 sets out the options available to the Court of Appeal when a party is not present when an appeal is called on for hearing. The options include, among others, ordering that the hearing not proceed unless other steps directed by the Court of Appeal are taken; adjourning the hearing; or proceeding with the hearing, either generally or in relation to the judgment sought in the appeal.

121 See Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, [13.2].

> It is a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and the defence. … Article 6 [of the European Convention on Human Rights][122] requires … that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused …
>
> However, … the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses at risk of reprisal or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused … [123]

7.65 The ECHR found that there was a breach of Article 6 of the European Convention on Human Rights caused by the action of the prosecution in deciding to withhold certain evidence during the applicant's trial on the grounds of public interest without notifying the judge. The ECHR found that the prosecution's failure to lay the evidence in question before the judge and allow him to rule on the question of disclosure deprived the applicants of a fair trial.[124] The ECHR noted that:

> the first instance judge would have been in a position to monitor the need for disclosure throughout the trial, assessing the importance of the undisclosed evidence at a stage when new issues were emerging, when it might have been possible through cross-examination seriously to undermine the credibility of key witnesses and when the defence case was still open to take a number of different directions or emphases.[125]

Open justice and national security information

7.66 The tension between principles of open justice and fair trials and the operation of mechanisms designed to protect classified information has been demonstrated in recent cases including the prosecution of former MI5 officer David Shayler, who was convicted for breaching the *Official Secrets Act 1989* (UK),[126] and the prosecution in the United States of Zacarias Moussaoui, an alleged conspirator in the attacks against the World Trade Centre and the Pentagon on 11 September 2001.

---

122 As stated in fn 9 and 76 above, Art 6(1) of the European Convention on Human Rights and its Five Protocols is in similar terms to Art 14(1) of the ICCPR. See Appendix 3 for the text of these Articles.

123 *Rowe and Davis v The United Kingdom* (2000) European Court of Human Rights Case no 28901/95, [60]–[61].

124 Ibid, [66].

125 Ibid, [65].

126 Shayler was convicted of disclosing documents, contrary to *Official Secrets Act 1989* (UK), s 1(1); disclosing documents obtained by interception of communications, contrary to *Official Secrets Act 1989* (UK), s 4(1); and disclosing documents purporting to relate to security or intelligence, contrary to *Official Secrets Act 1989* (UK), s 1(1). He was sentenced to six months' imprisonment on each count, to be served concurrently.

7.67 Shayler issued a statement that his conviction violated his right to a fair trial. He stated that he and his lawyers had been excluded from a number of secret hearings.[127] Shayler appealed to the Court of Appeal on the general ground:

> That the conviction is unsafe because the trial was conducted in breach of Article 6 of the European Convention on Human Rights, because the cumulative restrictions imposed upon the defendant deprived the proceedings of the character of an adversarial criminal trial and/or unfairly discriminated against him because he had chosen to defend himself.[128]

7.68 Shayler submitted that he was prejudiced by a number of restrictions placed on him in the presentation of his case,[129] including that he was limited in the cross-examination of an unnamed Security Services witness as to credibility and that he was required to disclose in advance to the prosecution all his evidence-in-chief and all his cross-examination areas and questions in detail.

7.69 The Court of Appeal dismissed Shayler's appeal. It stated that the cross-examination by Shayler was 'only restricted in accordance with well-established principle and to the extent that it would have been restricted if the applicant had been represented by counsel.'[130] The Court did not accept Shayler's submission concerning the regime imposed upon him requiring him to give advance notice of his case, holding that the ruling on advance notice was limited to any matter relating or purporting to relate to security or intelligence which he wished to raise.[131] The Court pointed to the trial judge's ruling that:

> If the defendant wishes to raise any matter relating or purporting to relate to security or intelligence, he must give the Court advance notice of that, be it raised in the form of questions to any witnesses or once the Crown case had closed, should it be necessary and the case go any further in relation to any evidence he wishes to adduce.[132]

The case against Moussaoui

7.70 In the US, the current proceedings against Zacarias Moussaoui case illustrate the particular difficulties in affording a self-represented accused[133] in a terrorist-related

---

127 *Freed Shayler Vows to Clear Name*, <www.guardian.co.uk/shayler/article/0,2763,864866,00.html> at 23 December 2002.

128 *R v Shayler* [2003] EWCA Crim 2218, [1].

129 Methods used to restrict the disclosure of evidence during Shayler's trial are discussed further in Ch 8.

130 *R v Shayler* [2003] EWCA Crim 2218, [27].

131 Ibid, [21].

132 Ibid, [21].

133 The question has been raised as to whether the right to defend oneself should apply in 'cases of extraordinary complexity involving large volumes of classified information' and the opinion expressed that 'Letting Mr Moussaoui represent himself has, in the name of liberty, reduced the chances of a fair and error-free trial. Congress should consider creating an exception to the right of self-representation for situations in which significant national-security barriers preclude even an able defendant from conducting a competent defense': Editorial, 'The Moussaoui Law', *Washington Post*, 4 August 2003, A14, <www.washingtonpost.com/ac2/wp-dyn/A17028-2003Aug3?language=printer>. In November 2003, the judge revoked Moussaoui's right to represent himself and appointed his standby attorneys to represent

trial all the guarantees of a fair trial while simultaneously safeguarding national security. Moussaoui was charged in December 2001 with conspiring with al-Qaeda in the terrorist attacks on the World Trade Center and the Pentagon. Moussaoui, an admitted al-Qaeda sympathiser has denied involvement in the attacks. The trial judge, Brinkema J, 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.[134] Prosecutors unsuccessfully challenged a court order allowing Moussaoui access to Ramzi bin al-Shibh, an al-Qaeda prisoner held in secret detention alleged to have information important to the defence, on the basis that such access could harm a sensitive key interrogation and threaten national security.[135] The US Department of Justice refused to make the al-Qaeda prisoner available for testimony in order to protect classified material.[136] The Department also indicated that it would not comply with a court order granting Moussaoui access to a further two al-Qaeda operatives being held at an undisclosed location.[137]

7.71 If the case were moved to a military tribunal, Moussaoui would not have the right to interview the witnesses. The defence applied for a dismissal of the case against Moussaoui on the basis that the Government's failure to produce the key witnesses would prevent Moussaoui from receiving a fair trial.[138] Moussaoui contended that to stop bin al-Shibh from testifying would violate the US Constitution.[139]

7.72 In October 2003, Brinkema J removed the death penalty as a possible sentence for Moussaoui and barred the use of any evidence relating to his involvement in the attacks on 11 September 2001.[140] She declared that:

---

him: J Markon, *Lawyers Restored for Moussaoui*, <www.washingtonpost.com/ac2/wp-dyn/A41492-2003Nov14?language=printer> at 15 November 2003.

134 *Moussaoui Crafts a Defense as Judge Appears to Listen*, <www.courttv.com/trials/moussaoui/042303_defense_ap.html> at 23 April 2003.

135 *Moussaoui Can Be Tried in Civilian Court*, <www.courttv.com/trials/moussaoui/041503_ap.html> at 15 April 2003 and J Markon, *Moussaoui Judge Rejects US Offer*, <www.washingtonpost.com/ac2/wp-dyn/A51670-2003Sep9?language=printer> at 10 September 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> at 26 June 2003.

136 P Shenon, *US Will Defy Court's Order in Terror Case*, The New York Times, <www.nytimes.com/2003/07/15/politics/15SUSP.html> at 15 July 2003.

137 J Markon, *US Refuses to Produce Al Qaeda Officials as Witnesses*, <www.washingtonpost.com/ac2/wp-dyn/A56579-2003Sep10?language=printer> at 11 September 2003.

138 J Markon, *Defense Calls for Dismissal of Sept 11 Case*, <www.washingtonpost.com/ac2/wp-dyn/A60716-2003Sep24?language=printer> at 25 September 2003.

139 J Markon, *Moussaoui Judge Rejects US Offer*, <www.washingtonpost.com/ac2/wp-dyn/A51670-2003Sep9?language=printer> at 10 September 2003. The Sixth Amendment to the US Constitution gives the accused in a criminal prosecution the right 'to have compulsory process for obtaining witnesses in his favor'. See Appendix 3 for the full text.

140 The US Government could, however, pursue charges that Moussaoui participated in a broad al-Qaeda conspiracy to attack the United States.

> the Government will be foreclosed at trial from making any argument, or offering any evidence, suggesting that the defendant had any involvement in, or knowledge of, the September 11 attacks. It would simply be unfair to require Moussaoui to defend against such prejudicial accusations while being denied the ability to present testimony from witnesses who could assist him in contradicting those accusations.[141]

7.73 In light of these sanctions, Brinkema J stated that the Court was no longer satisfied that the testimony from the al-Qaeda operatives was material to Moussaoui's defence and therefore concluded that his right to a fair trial was no longer offended by the Government's refusal to comply with her court orders relating to access to the operatives.[142]

7.74 In rejecting the application for outright dismissal of the charges, Brinkema J commented that:

> The unprecedented investment of both human and material resources in this case mandates the careful consideration of some sanction other than dismissal … Finding that this case can be resolved in an open and public forum, the Court concludes that the interests of justice would not be well served by dismissal.[143]

Abuse of process

7.75 In taking measures to ensure that a trial is fair, courts may 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.[144] Where proceedings are temporarily (as opposed to permanently) stayed or lesser charges than those contained in the indictment are proceeded with, the prosecution may pursue the original charge on the indictment at a later date without compromising the accused's right not to be subject to double jeopardy.[145] An adjournment or temporary stay, rather than a dismissal or permanent stay, could be appropriate in circumstances where the sensitivity of the information might not be ongoing.[146]

7.76 These powers can be applied in cases involving classified or security sensitive information in court proceedings. For example, in the prosecution of Simon Lappas 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

---

141 *United States v Moussaoui* (Unreported, US District Court for the Eastern District of Virginia, Brinkema J, 2 October 2003), 13.

142 Ibid, 13.

143 Ibid, 5. At the time of writing the US Court of Appeals for the 4th Circuit was hearing oral arguments in the US Government's appeal against Brinkema J's ruling. The Court has raised the prospect that it 'might order, or even draft, a compromise that would allow Moussaoui access to statements made by three key al Qaeda detainees without letting him or his attorneys interview the witnesses in person': J Markon, *Compromise Hinted in Moussaoui Case*, <www.washingtonpost.com/ac2/wp-dyn/A33105-2003Dec3?language=printer> at 4 December 2003.

144 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 536.

145 Art 14(7) of the ICCPR protects an accused from double jeopardy. Art 14(7) is set out in Appendix 3.

146 Australian Federal Police, *Submission CSSI 13*, 18 September 2003.

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.[147] 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.[148]

7.77 Gray J 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.[149]

7.78 It was central to the Crown's 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.[150] Gray J 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, but that it also seemed to prevent the prosecution from adducing evidence highly relevant to its own case.[151]

7.79 Gray J's decision that the trial could not be conducted fairly without the jury (as the trier of fact) seeing the documents was open to him in the circumstances of the case and would be equally open to another trial judge faced with a similar situation. However, exposure of the documents to the jury may well have constituted a more

---

147 *R v Lappas and Dowling* [2001] ACTSC 115. 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. See Appendix 4 for a discussion of the case.

148 *R v Lappas and Dowling* [2001] ACTSC 115, [14].

149 Ibid, [24].

150 Ibid, [21].

151 Ibid, [18]–[19].

serious security breach than that which had led to the charges being laid given that the documents had never reached the foreign power for which they were intended.[152]

7.80 A defendant denied access to classified or security sensitive documents upon which the prosecution relies may argue that the right to a fair trial is compromised because of that denial and the defendant's consequent inability to challenge or test part of the evidence. The burden of proving that the proceedings amount to an abuse of process falls on the accused.[153] 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. However, a stay is only to be ordered in exceptional cases.[154]

7.81 In the United States, the *Classified Information Procedures Act* (CIPA) provides that, if the US 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.[155] 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.[156]

Procedural protections in non-criminal proceedings

7.82 As stated above, some basic procedural protections guaranteed by international law apply exclusively to criminal proceedings. In *Detroit Free Press v John Ashcroft*,[157] the US 6th Circuit Court of Appeals 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* [sic] *Group, Inc. v Ashcroft,* 205 F.Supp 2d 288, 301 (DNJ2002). '[D]eportation can be the equivalent of banishment or exile,' *Delgadillo v*

152 Advisory Committee member, *Correspondence*, 18 September 2003.
153 *Tan v Cameron* [1992] 2 AC 206.
154 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 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; *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).
155 See discussion on CIPA in Ch 8 at [8.55]–[8.76].
156 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(e).
157 *Detroit Free Press v Ashcroft* (Unreported, US Court of Appeals for the 6th Circuit, Keith and Daughtrey (Circuit Judges) Carr (District Judge), 26 August 2002), 12.

> *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.

7.83 In light of the serious consequences that flow from deportation and other similar proceedings, the question arises about what basic 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.[158]

7.84 The Law Society of New South Wales submitted that:

> In similar terms to criminal proceedings, immigration proceedings may impact on the freedom of an individual and persons facing immigration proceedings which could result in their removal from Australia should be afforded similar protections as provided to people in criminal trials.[159]

7.85 The Human Rights and Equal Opportunity Commission (HREOC) noted in its submission that decisions in immigration and similar hearings involving classified or security sensitive information may affect a person's rights to liberty under Article 9 of the ICCPR, or the right to leave any country (including their own) under Article 12(2) of the ICCPR.[160] HREOC submitted that it would be desirable to have further specific procedural guarantees in these hearings.[161]

7.86 The right to certain basic procedural protections can also be found in international instruments dealing with non-criminal proceedings. Article 32 of the Convention Relating to the Status of Refugees (the Refugee Convention) 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

158 The use of secret evidence and secret hearings in non-criminal matters is discussed in Ch 9.

159 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

160 Art 9(1) of the ICCPR provides that 'Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedures as are established by law.' Art 12(2) of the ICCPR provides that 'Everyone shall be free to leave any country, including his own.'

161 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003.

> before competent authority or a person or persons specially designated by the competent authority.[162]

7.87 Australia is bound by Article 32 of the Refugee Convention[163] as well as Article 13 of the ICCPR, which, although not limited to refugees, is in similar terms to Article 32, stating:

> 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.

7.88 The requirement that people facing expulsion be allowed to submit evidence carries an implicit requirement that they be allowed to know the case for expulsion.[164]

> 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.[165] …
>
> For this reason, too, it is not conducive to the making of correct decisions to keep adverse material secret.[166]

7.89 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.[167]

---

162 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'.

163 The Australian Government had made a reservation with respect to Article 32 of the Convention but that reservation was withdrawn on 1 December 1967.

164 S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 404–405.

165 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.

166 S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 405.

167 Ibid, 406.

7.90 Article 1F of the Refugee Convention provides that the provisions of the Convention do not apply to any person with respect to whom there are serious reasons for considering that:

> (a) He has committed a crime against peace, a war crime, or a crime against humanity, as defined in the international instruments drawn up to make provision in respect of such crimes;
>
> (b) He has committed a serious non-political crime outside the country of refuge prior to his admission to that country as a refugee;
>
> (c) He has been guilty of acts contrary to the purposes and principles of the United Nations.

7.91 The Guidelines of the United Nations High Commissioner for Refugees on the application of Article 1F provide that:

> Exclusion should not be based on sensitive evidence that cannot be challenged by the individual concerned. Exceptionally, anonymous evidence (where the source is concealed) may be relied upon but only where this is absolutely necessary to protect the safety of witnesses and the asylum seeker's ability to challenge the substance of the evidence is not substantially prejudiced. Secret evidence or evidence considered in camera (where the substance is also concealed) should not be relied upon to exclude. Where national security interests are at stake, these may be protected by introducing procedural safeguards which also respect the asylum-seeker's due process rights.[168]

7.92 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'; and

- 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',[169] 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'.[170]

---

168 United Nations High Commissioner for Refugees, *Guidelines on International Protection: Application of the Exclusion Clauses: Article 1F of the 1951 Convention Relating to the Status of Refugees*, 4 September 2003, [36].

169 Refugee Convention, Art 33(1).

170 Ibid, Art 33(2).

The right to a public judgment

7.93 One important aspect of the right to a public trial is the right to a public judgment,[171] which ensures that the administration of justice is open and subject to public scrutiny. This right extends to judgments rendered by all courts, including special and military courts and courts of appeal.[172]

7.94 The right to a public judgment has been interpreted to require courts to provide reasons for their judgments. The right to receive judgment is essential to the right of the accused to appeal.[173] The right to a fair hearing encompasses the right to a statement of reasons for a judgment,[174] 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.

7.95 A judgment is public if it is delivered orally in a court session that is open to the public or if a written judgment is published.[175]

> The right to a public judgment is violated if judgments are made accessible only to a certain group of people or when only people having a specific interest are allowed to inspect a judgment. … The requirement that judgments be made public (in all but the exceptional circumstances …) applies even if the public has been excluded from all or parts of the trial.[176]

171 See ICCPR, Art 14 set out in Appendix 3. See also *International Criminal Court Act 2002* (Cth), Sch 1, Art 74(5), which provides for a written 'full and reasoned statement of the Trial Chamber's findings on the evidence and conclusions' and that the 'decision or a summary thereof shall be delivered in open court.'

172 Amnesty International, *Amnesty International Fair Trials Manual*, <www.amnesty.org/ailib/intcam/fairtrial/fairtria.htm>, [24.1].

173 Ibid, [24.2]. The Human Rights Committee found in a case where a Jamaican appeals court failed to issue a reasoned written judgment that the accused's rights had been violated because the failure was likely to prevent the accused from successfully arguing for special leave to appeal to a higher tribunal and therefore from availing himself of an additional remedy: *Hamilton v Jamaica*, (333/1988), 23 March 1994, UN Doc CCPR/C/50/D/333/1988, 1994, 5–6.

174 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.

175 See also, for example, *Supreme Court Rules 1970* (NSW), Part 40, r 2 which provides that 'Where the Court gives any judgment or makes any order and the opinion of the Court or of any Judge or officer of the Court is reduced to writing, it shall be sufficient to state orally the opinion of the Court, Judge or officer without stating the reasons for the opinion, but the written opinion shall be then given by delivering it to an associate or to the registrar or to an officer of the registry'.

176 Office of the High Commissioner for Human Rights, *Equality Before the Courts and the Right to a Fair and Public Hearing by an Independent Court Established by Law (Art 14): 13/04/84. CCPR General Comment 13*, <www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+13.En?OpenDocument/> [6].

7.96 The UN Human Rights Committee has similarly held that 'even in cases in which the public is excluded from the trial, the judgment must, with certain strictly defined exceptions, be made public.'[177]

7.97 For example, the *Official Secrets Act 1989* (UK), which applies the provisions of the *Official Secrets Act 1920* (UK) in relation to hearings closed on the grounds of national security, specifically provides that 'the passing of sentence shall in any case take place in public.'[178]

7.98 In *R v Tait and Bartley*, the Full Court of the Federal Court of Australia stated:

> Where a court is authorized to sit in camera and does so sit, or where it receives documents the contents of which are not published … it will usually be desirable to say so in the published reasons for judgment. … Where in these exceptional cases, the court is limited in expressing its reasons for according confidentiality to proceedings or to the contents of documents, because an expression of reasons may destroy the confidentiality which is seen to be necessary, it is desirable to ensure that the unpublished material furnished to the court is kept suitably in the registry in order that the foundation upon which the court has acted may be examined either by an appeal court or by a member of the public who is able to persuade the court to revoke or vary the order prohibiting public access to that material.[179]

7.99 In *Grant v Headland*, after conducting appeal proceedings in camera to ascertain the national security quality of information which was passed by a junior intelligence trainee convicted under s 79(3) of the *Crimes Act 1914* (Cth),[180] Smithers J delivered a public judgment stating:

> I have written these reasons for delivery in open court. They state my conclusions on the security aspect of the matter. The precise content of the information attempted to be communicated has been omitted, but so far as the interests of the appellant are concerned, they do not suffer in this, as I have accepted the argument of his counsel as to the security significance thereof.[181] I have adopted this course to reconcile the appellant's desire for as much openness as possible with the view that it would be prejudicial to the interests of justice that proceedings in which matters of security were involved entailed unnecessary publication of security operations.[182]

7.100 In *The Attorney General of Canada and Nicholas Ribic and The Attorney General of Ontario*, in determining an application by the Attorney General of Canada

---

177 Ibid, [6].

178 See *Official Secrets Act 1920* (UK), s 8(4); *Official Secrets Act 1989* (UK), s 11(4). The provisions in the *Official Secrets Acts* dealing with closed hearings are discussed in Ch 8.

179 *R v Tait and Bartley* (1979) 24 ALR 473, 492, where the Court observed that 'the absence of a written record of the discussions in chambers led to a chain of undesirable consequences—[including] an appeal argued on the footing that no relevant material had been furnished in chambers [and] subsequent disagreement between the parties as to the material which had been furnished'.

180 See discussion of this case in Ch 8 under the heading 'Closing courts to the public'.

181 After considering the evidence in camera, Smithers J found that the security significance of the information was minor.

182 *Grant v Headland* (1977) 17 ACTR 29, 34.

under s 38 of the *Canada Evidence Act*, Lutfy ACJ of the Federal Court of Canada stated that:

> These reasons for order have been written with the view of not disclosing the secret information and, to the extent possible, the evidence and representations in the *ex parte* sessions and some of the arguments of counsel for the respondent Ribic.[183]

7.101 In some cases, it may be appropriate for full reasons for judgment to be released at a later time when the sensitivity of the material is reduced or is no longer an issue. For example, *In the Matter of an Application Under s 83.28 of the Criminal Code and The Vancouver Sun*,[184] Holmes J publicly released a synopsis of the in-camera proceedings which provided a broad outline of the proceedings and their outcome. Her Honour stated that the full reasons for judgment, which involved a more extensive discussion of the issues and the underlying facts, were sealed and would be released after the completion of the investigative hearing, and she noted the possibility that other material relating to the in-camera proceedings might be able to be released at that time.[185]

7.102 In *Re Criminal Proceeds Confiscation Act 2002 (Qld)*, a case which considered judicial power and judicial process under Chapter III of the *Australian Constitution*,[186] White J of the Queensland Court of Appeal stated:

> Accepting that there may be occasions, particularly in interlocutory proceedings, when it will not be necessary for a judicial officer to give detailed reasons, for example, in arguments about the provision of particulars, it should be regarded generally as a normal incident of the judicial process; [citations omitted] …
>
> It has been said the obligation to give reasons is to enable the case to be 'properly and sufficiently' laid before the higher appellate court, *Pettitt v Dunkley* [1971] 1 NSWLR 376 at 388. Making an order ex parte seems to me similarly to be a case where the party adversely affected by the order as well as any subsequent court hearing the matter, needs to know the basis upon which a court exercised its discretion or was satisfied that the legislative conditions for making the order had been met. … No matter how brief, record of what the court had regard to seems a necessary aspect of the judicial process.[187]

7.103 There are numerous instances in Australian administrative procedures where the right of either the public or of the applicant or affected person to a full statement of

---

183 *The Attorney General of Canada and Nicholas Ribic and The Attorney General of Ontario* (2002) FCT 839. This case is discussed further in Ch 8 at [8.93]–[8.94]. Note also that in the United States a judge of the Alien Terrorist Removal Court who denies an order sought in an application filed by the Attorney General for the removal of an alien where the Attorney General has classified information that the alien is a terrorist, must 'prepare a written statement of the reasons for the denial, taking all necessary precautions not to disclose any classified information contained in the Government's application.' See 8 USC (US), s 1533(1) and (3). The Alien Terrorist Removal Court is discussed further in Ch 9.

184 Discussed at [7.29]–[7.33] above.

185 See *In the Matter of an Application under s 83.28 of the Criminal Code and The Vancouver Sun* (2003) BCSC 1330, [16], [29].

186 See the discussion of Chapter III issues in Ch 9.

187 *Re Criminal Proceeds Confiscation Act 2002 (Qld)* [2003] QCA 249, [62]–[63].

reasons is qualified or removed. Where the Security Appeals Division of the Administrative Appeals Tribunal (AAT) conducts a review, it may publish an open decision, which is given to the applicant, and a closed decision, which is classified.[188] The Security Appeals Division is obliged to record its findings in relation to a security assessment.[189] It must provide copies of its findings to the applicant, the Director-General of Security, the agency to which the assessment was given and the Attorney-General,[190] except that it may:

> direct that the whole or a particular part of its findings, so far as they relate to a matter that has not been already disclosed to the applicant, is not to be given to the applicant or is not to be given to the Commonwealth agency to which the assessment was given.[191]

7.104 The AAT Act also provides that in relation to proceedings before the Security Appeals Division to which s 39A applies—being proceedings involving the review of a security assessment—the AAT may give directions prohibiting or restricting the publication of 'the whole or any part of its findings on the review'.[192]

7.105 The Australian Security Intelligence Organisation (ASIO) is required to provide a statement of its grounds for an adverse or qualified security assessment of Australian citizens or permanent residents which contains all information relied upon by ASIO in making the assessment, except information the inclusion of which would, in the opinion of the Director-General of Security, be contrary to the requirements of security.[193] The Attorney-General may certify that he or she is satisfied that it is essential to national security to withhold notice to a person of the fact of the making of a security assessment.[194] A statement of grounds may also 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.[195] If the Attorney-General has made such a certification, the AAT in conducting a review of the security assessment is precluded from disclosing the document to the applicant.[196] The Federal Court is also precluded from disclosing the document in considering an appeal of the AAT decision.[197]

---

188 Concern has been expressed that proper internal procedures are not in place to ensure that the closed decision is not mistakenly released to the applicant: Advisory Committee members, *Advisory Committee meeting*, 19 September 2003.

189 *Administrative Appeals Tribunal Act 1975* (Cth), s 43AAA(2).

190 Ibid, s 43AAA(4).

191 Ibid, s 43AAAA(5).

192 Ibid, s 35AA(d).

193 *Australian Security Intelligence Organisation Act 1979* (Cth), s 37(2)(a).

194 Ibid, s 38(2)(a). This denies the affected person knowledge of the fact that a decision has been made, not just the grounds for the decision.

195 Ibid, s 38(2)(b).

196 *Administrative Appeals Tribunal Act 1975* (Cth), s 39B.

197 Ibid, s 46.

7.106 The *Service and Execution of Process Act 1992* (Cth) provides that, upon application, a magistrate or court[198] may order that the report of a finding publicly made by the magistrate or court is not to be published if satisfied that publication of the report would give rise to a substantial risk that national security would be prejudiced.[199]

7.107 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.'[200] Similarly, under the *Anti-Terrorism, Crime and Security Act 1981* (UK), the Lord Chancellor may make rules that 'provide for full particulars of the reasons for denial of access to be withheld from the applicant and from any person representing him'.[201] Under the *Terrorism Act 2000* (UK), which allows the Secretary of State to proscribe organisations concerned in terrorism and for an appeal to be made to the Proscribed Organisations Appeal Commission,[202] the Lord Chancellor is empowered to make rules which:

> provide for full particulars of the reasons for proscription or refusal to deproscribe to be withheld from the organisation or applicant concerned and from any person representing it or him; … [203]

7.108 The *Regulation of Investigatory Powers Act 2000* (UK) allows the Secretary of State to make rules:

> enabling or requiring the [Investigatory Powers] Tribunal[204] to exercise their jurisdiction, and to exercise and perform their powers and duties conferred or imposed on them (including, in particular, in relation to the giving of reasons), in such manner provided for in the rules as prevents or limits the disclosure of particular matters.[205]

7.109 In making any such rules, the Secretary of State must have regard to:

> the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or

198 Being the Supreme Court of a State conducting a review under the *Service and Execution of Process Act 1992* (Cth), s 86.
199 Ibid, s 96(2) and (3)(f).
200 *Special Immigration Appeals Commission Act 1997* (UK), s 5(3)(a).
201 *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.
202 *Terrorism Act 2000* (UK), s 3 and 5. See also discussion on POAC under heading 'Tribunals closed to a party' in Ch 9.
203 Ibid, Sch 3, 4(a).
204 The Investigatory Powers Tribunal was set up to investigate complaints about the intelligence services or relating to the interception of communications and is discussed further in Ch 2.
205 *Regulation of Investigatory Powers Act 2000* (UK), s 69(4)(d).

> detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the function of any of the intelligence services.[206]

7.110 Rule 13(2) of the *Investigatory Powers Tribunal Rules 2000* (UK) only requires the Tribunal, where it has made a determination in favour of a complainant, to provide the complainant with a summary of that determination including any findings of fact, rather than full reasons for the determination. The Tribunal's duty to provide such a summary is subject to its general duty to carry out its functions in such a way as to ensure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the function of any of the intelligence services.[207]

7.111 If no determination is made in favour of the complainant, there is no entitlement to receive any more than notification of that fact.[208] Where the Tribunal makes certain determinations against the complainant, including that the complaint is frivolous or vexatious, that the complaint has been made out of time or that the complainant does not have the right to make the complaint, the Rules require the Tribunal to notify the complainant of that fact only.[209]

7.112 In a recent case where r 13(3) of the *Investigatory Powers Tribunal Rules 2000* was challenged, the Tribunal held that, so far as determinations were concerned, it was satisfied that r 13 and s 68(4) of the *Regulation of Investigatory Powers Act 2000* (UK) were valid and binding and 'that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the [neither confirm nor deny] policy[210] must be preserved) is necessary and justifiable.'[211] The Tribunal held that r 13 and s 68(4) did not apply to prevent publication of the Tribunal's reasons for rulings on preliminary issues of procedural law as these did not constitute a 'determination' of the proceedings brought before it as such rulings did not determine the merits of the claim or bring the proceedings to an end.[212]

Consultations and submissions

7.113 In BP 8, the ALRC asked whether there should be any limitation on the publication of written reasons for any judgment or decision in proceedings involving classified or sensitive material, including where such evidence has been led in in-camera pro-

---

206 Ibid, s 69(6)(b).
207 *Investigatory Powers Tribunal Rules 2000* (UK), rule 6(1).
208 *Regulation of Investigatory Powers Act 2000* (UK), s 68(4)(b).
209 *Investigatory Powers Tribunal Rules 2000* (UK), r 13(3).
210 This is a reference to the policy of public authorities in response to questions asked or complaints made about interception and surveillance to neither confirm nor deny whether the alleged activities have occurred or are still occurring: *In the Investigatory Powers Tribunal In Camera—In the Matter of Applications Nos IPT/01/62 and IPT/01/77—Draft Rulings of the Commission on Preliminary Issues of Law*, 23 January 2003, [47].
211 Ibid, [191].
212 Ibid, [190]–[191].

ceedings or has been the subject of non-publication orders imposed by the court.[213] The ALRC also asked whether there should 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.[214]

7.114 The Law Society of NSW submitted that:

> Full reasons for any judgment or decision should be prepared. However, in extraordinary and limited circumstances where the public interest (including for reasons of national security) requires, a modified set of reasons, which at least set out the findings made, should be given to the affected party and subject to such further restrictions on further publication as the presiding judicial officer or decision maker considers appropriate.[215]

7.115 HREOC submitted that:

> [I]n most cases, judges and tribunals can give adequate reasons which indicate the classified information relied upon, without disclosing the nature of that classified information in the judgment or decision. Provided that such reasons still allow the judgment or decision to be reviewed in accordance with the right to review of a decision under Article 14(5) [of the ICCPR],[216] the requirements of the ICCPR will be met. It will be a question of drawing an appropriate balance in each case.[217]

7.116 The Australian Press Council submitted that:

> The suggestion that judicial officers should not give reasons for decisions is plainly repugnant. More problematic is the notion that reasons should not be available to the public. Suppression orders are already used by courts to protect the identities of minors in certain proceedings, notably where child sexual assault is involved. More commonly, only the identities of witnesses, victims or defendants are suppressed but the judgment is otherwise published in full. Where proceedings concern matters of public interest, it would be inappropriate to remove judicial reasoning from public scrutiny. The Press Council opposes the limiting of public access to judicial reasons where proceedings concern government action. If judicial officers do restrict publication of their reasons, they should prepare an edited version of their reasons and make this available to the public and the media.[218]

7.117 The ALRC's proposal in relation to the preparation of statements of reasons appears in Chapter 10 as part of the overall proposed new statutory regime governing the use of classified and security sensitive information in courts and tribunals. The ALRC's preliminary view is that in proceedings involving classified or security sensitive information, courts and tribunals should always prepare full written statements of reasons for any decision, including any authorised by the proposed new Act. However,

---

213 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 41.
214 Ibid, Q 43.
215 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.
216 See Appendix 3 for the text of ICCPR, Art 14(5).
217 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003.
218 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

the court or tribunal may, in its discretion, decide to publish an edited version of the statement of reasons to protect classified or security sensitive information. The version of the statement of reasons provided to any party whose interests might be adversely affected by the decision should be sufficient to allow that party to appeal the decision (where an avenue of appeal remains available).

8. Courts—Restricting Public Access

Contents

Introduction

8.1 The issue of protecting classified and security sensitive information arises in both criminal and civil proceedings, as well as in administrative proceedings before tribunals. This chapter considers the use of methods to restrict access to such information by the public while Chapter 9 considers the more controversial use of methods to restrict access to such information by the party affected.

8.2 Criminal proceedings in which the protection of classified and security sensitive information may be an issue include prosecutions of alleged acts of terrorism or espionage. Civil proceedings in which the protection of such information may be an issue include claims:

- brought against a government department or agency by, for example, members of the defence forces, intelligence personnel or their dependents or estates;[1]

- 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.

8.3 Administrative proceedings in which the use of classified or security sensitive information may arise include immigration proceedings and reviews of adverse security assessments.

Pre-trial procedures

Introduction

8.4 Classified or security sensitive information may emerge during the investigation or pre-trial stages of a matter as part of the processes of discovery and disclosure, as well as during the presentation of evidence during court and tribunal proceedings. Admission of evidence covers both oral testimony and the tendering of documents (broadly defined) and other exhibits. A distinction can be drawn between mechanisms to protect sensitive evidence and mechanisms to protect the *source* of sensitive evidence. This does not appear to lead to any difference in principle, but is rather just one of the variables to be taken into consideration by the court or tribunal in determining how to proceed.[2]

8.5 In criminal proceedings, the prosecution has an 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'.[3] An accused person does not carry any comparable general obligation of disclosure on the basis that the prosecution is required to prove its case without assistance from the defence. However, there are some specific obligations of disclosure imposed on the accused in most jurisdictions in Australia, and these are considered in Chapter 10.

---

1 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.

2 One view expressed in consultation was that protecting information and protecting the source of that information are often very closely connected. Revealing one may almost certainly reveal the other: B Leader, *Consultation*, By telephone, 26 August 2003.

3 Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/prosecutions/disclosure/>, E2.

8.6 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. However, it might have the effect (or purpose) of 'greymail'—that is, presenting the Government with the choice of either risking disclosure of the classified information or dismissing or compromising the indictment or charges.

8.7 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 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?

- How should classified and security sensitive information be handled in civil proceedings in pre-trial procedures where parties are under an obligation to discover all relevant documents (except where privilege attaches) to each other and may be obliged to answer interrogatories?

- How can unexpected evidence or evidence from third parties, especially during trial, be handled?

8.8 In considering the various methods used to restrict access to classified and security sensitive information, it is convenient to distinguish between those methods which are used either in the pre-trial stages of a matter or during court and tribunal proceedings, and those which are or could be used both pre-trial and in court.

Pre-trial methods

Withholding material from suspects

8.9 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.[4] Section 23V(1) makes a confession or admission of a person interviewed

4 Section 23V is set out in full in Appendix 3.

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,[5] 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.[6] 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.[7]

8.10 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.[8] 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.[9]

8.11 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,[10] or if it is satisfied that it was not practicable to comply with the section.[11] 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.[12] These provisions could be relevant to the current inquiry although not as specifically relevant as s 23V(3) 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.

8.12 The Australian Crime Commission submitted that:

> The question of preventing disclosure of information to suspects in order to protect covert investigations and related information is particularly relevant to the ACC which uses a range of covert investigation methods, and which may conduct its investigations jointly with other agencies, and which maintains the national criminal intelligence database. Since the ACC is primarily interested in major criminal identities and networks, the short term benefits of proceeding with a prosecution to secure conviction of minor offences will usually be outweighed by the longer term benefits

---

5 *Crimes Act 1914* (Cth), s 23V(1)(a).
6 Ibid, s 23V(1)(b).
7 Ibid, s 23V(1)(b).
8 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).
9 *Lai-Ha v McCusker* [2000] FCA 1173 (Emmett J).
10 *Crimes Act 1914* (Cth), s 23V(5).
11 Ibid, s 23V(6).
12 Ibid, s 23V(7).

> of gaining convictions of the major criminals and ensuring longer-term intelligence production to guide broader policy enhancement. In all such cases, however, case-by-case variables need to be closely examined.[13]

8.13 The Attorney-General's Department raised the issue of whether Australia's investigating agencies should be permitted to withhold recordings and transcripts of confessions and admissions from suspects where they involve national security information. It stated that any reform of s 23V of the *Crimes Act 1914* (Cth) to meet security requirements should continue to fulfil the purpose of s 23V, which was to 'provide a disincentive against the manufacture of false statements.'[14] However, the Attorney-General's Department did not express any views on whether s 23V should be amended to allow the withholding of recordings and transcripts of confessions and admissions on the ground of national security.

8.14 No other submissions were received in relation to the operation or potential reform of s 23V nor on the current practices of investigating agencies 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.[15] No information was brought to the ALRC's attention to suggest that s 23V is not currently working well. In the circumstances, the ALRC does not make any proposal in this regard. However, the ALRC remains interested in hearing further submissions in relation to the possible need for reform of s 23V.

Detention and restrictions on communications

8.15 The *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Cth) made a number of amendments to the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) which have the effect of protecting security sensitive information relating to the investigation of terrorism offences.[16] The Act does not refer to security sensitive information. However, it does define 'operational information' and establishes offences for the unauthorised disclosure of such information.[17] Its principal intention is to enhance 'the capacity of ASIO to exercise its powers for questioning and detaining persons who have information important to the gathering of intelligence in relation to a terrorism offence.'[18] However, the fact that an investigation is being undertaken by ASIO is likely of itself to constitute security sensitive information.

---

13 Australian Crime Commission, *Submission CSSI 15*, 13 October 2003.

14 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

15 See Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 44.

16 A 'terrorism offence' is defined as an offence against Division 72 or Part 5.3 of the *Criminal Code*: *Australian Security Intelligence Organisation Act 1979* (Cth), s 4. See discussion on ASIO in Ch 2.

17 See [8.20] below.

18 *ASIO Legislation Amendment Bill 2003 Explanatory Memorandum*.

8.16 The ASIO Act limits the contact that a person in custody can have:

> A person who has been taken into custody, or detained, under this Division is not permitted to contact, and may be prevented from contacting, anyone at any time while in custody or detention.[19]

8.17 The ASIO Act specifically provides that a person may be prevented from contacting a particular lawyer of choice if the prescribed authority so directs.[20] However, the prescribed authority may only give such a direction if it is satisfied, on the basis of circumstances relating to that lawyer, that, if the person is allowed to contact that lawyer:

> (a) a person involved in a terrorism offence may be alerted that the offence is being investigated; or
>
> (b) a record or thing that the person may be requested in accordance with the warrant to produce may be destroyed, damaged or altered.[21]

8.18 Where a person contacts a legal adviser as permitted by the warrant, or under a direction given by the prescribed authority, the ASIO Act provides that:

> The contact must be made in a way that can be monitored by a person exercising authority under the warrant.[22]

8.19 The view has been expressed that 'denial of access to independent and freely chosen legal advice and representation while in detention may, in particular, infringe on [the implied right in the *Australian Constitution* to] political communication'.[23]

8.20 Amendments made to the ASIO Act in December 2003 aim to protect the effectiveness of intelligence gathering operations by

- preventing a person from making a primary or secondary disclosure of information without authorisation where the information relates to the warrant, the questioning or detention of a person under the warrant, or operational information while the warrant is in force, and

---

19 *Australian Security Intelligence Organisation Act 1979* (Cth), s 34F(8). However, the person may contact anyone whom the warrant allows him or her to contact, or whom the prescribed authority, by direction, allows him or her to contact. Further, the Act allows certain contact between the person and the Inspector-General of Intelligence and Security, and the Ombudsman: *Australian Security Intelligence Organisation Act 1979* (Cth), s 34F(9).

20 *Australian Security Intelligence Organisation Act 1979* (Cth), s 34TA(1).

21 Ibid, s 34TA(2). This does not prevent the person from choosing another lawyer to contact, although the person could also be prevented from contacting that lawyer on the same basis: *Australian Security Intelligence Organisation Act 1979* (Cth), s 34TA(4). Section 34TB provides, for the avoidance of doubt, that a person may be questioned under a warrant issued under the Act before a prescribed authority in the absence of a lawyer of the person's choice: *Australian Security Intelligence Organisation Act 1979* (Cth), s 34TB.

22 *Australian Security Intelligence Organisation Act 1979* (Cth), s 34U(2).

23 See M Head, ''Counter-Terrorism' Laws: A Threat to Political Freedom, Civil Liberties and Constitutional Rights' (2002) 26(3) *Melbourne University Law Review* 666, 687–688.

- preventing a person from making a primary or secondary disclosure of operational information without authorisation for two years after the warrant ceases to be in force.[24]

8.21 Although it is interesting to note these provisions as examples of methods invoked to protect classified and security sensitive information, the ALRC does not intend to make any proposals in relation to these aspects of the ASIO Act. Any review of these provisions should be undertaken in conjunction with a review of the Act's scheme in relation to the detention and interrogation of suspects and other witnesses as a whole, which is clearly outside the Terms of Reference for this inquiry.

Presenting evidence in open court

Introduction

8.22 The principal techniques that can be used to block the admission into evidence of classified and security sensitive information are claims for public interest immunity and the use of ministerial certificates exempting material from production or prohibiting its disclosure. These are discussed at [8.118] and [8.183] below. The following discussion deals with ways of admitting or leading classified evidence. The discussion is divided into four sections. The first considers methods that can be used both in pre-hearing processes such as discovery and disclosure as well as in court; the second section deals with additional methods used in court to present sensitive evidence;[25] the third section discusses methods used to protect confidential sources of information; and the fourth section considers the legislative schemes in the United States, the United Kingdom and Canada dealing with classified and security sensitive information.

Methods used both pre-trial and in court

8.23 Some mechanisms limiting the disclosure or discovery of classified or security sensitive information before trial can also 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;[26]
- substituting a statement admitting relevant facts that the classified information would tend to prove;[27]

---

24 Attorney-General, *ASIO Changes Through Parliament*, Media Release, 5 December 2003. See *Australian Security Intelligence Organisation Act 1979* (Cth), s 34VAA(1) and (2), breaches of which attract a maximum penalty of five years' imprisonment.

25 Some of these methods are discussed more fully in later sections of this chapter.

26 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> at 1 June 2002.

- 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;[28]
- substituting an unclassified summary of the classified information;[29]
- issuing protective orders against disclosure and sealing orders;[30]
- issuing orders regarding custody and handling of information;[31] and
- using ex parte applications (ie, proceedings in the absence of one or more of the parties) for the protection of material from disclosure.

8.24 These techniques are aimed at permitting the sensitive material to be used securely or offering satisfactory substitute evidence to be admitted.

8.25 A claim for public interest immunity, which prevents the admission of evidence,[32] can also be made at the pre-trial stages of a matter—for example, in response to a subpoena for production of documents where the material produced includes classified or security sensitive information—as well as during court proceedings.

8.26 It is interesting to note that, while some of the methods are used or could be used in Australia, their availability to the courts and to the parties does not appear to be set out in any particular statute or subordinate rules. As discussed below, the *Classified*

---

27 The *Evidence Act 1995* (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. An 'agreed fact' is defined in s 191(1) as 'a fact that the parties to a proceeding have agreed is not, for the purposes of the proceeding, to be disputed'. Unless the court gives leave, evidence is not required to prove the existence of an agreed fact and evidence may not be adduced to contradict or qualify an agreed fact: *Evidence Act 1995* (Cth), s 191(2).

28 Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/prosecutions/disclosure/>, 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'.

29 See comments about declassified summaries in the discussion on secret evidence in Ch 9 at [9.2] and, in particular at [9.9].

30 For example, confidential sealing orders can be made to protect the names of informants. In *Attorney-General v Kaddour & Turkmani* [2001] NSWCCA 456, [23], the NSW Court of Criminal Appeal ordered that all copies of the Confidential Statements referred to in its judgment (which were exhibits to affidavits by two Deputy Police Commissioners making a public interest claim in relation to the identity of informers) 'be placed in a sealed envelope, the envelope being marked "*Confidential: not to be opened without the prior order of a Judge of this Court*"; and kept with the Court file for any necessary future reference.'

31 Australian Federal Police, *Submission CSSI 13*, 18 September 2003 and Advisory Committee members, *Advisory Committee meeting*, 19 September 2003.

32 See [8.118] below.

Information Procedures Act (US), the *Code of Practice* (UK) and the *Canada Evidence Act* provide for court-approved alternatives to full disclosure of sensitive material to an accused. However, there is no Australian legislative provision or court rule allowing an unclassified summary of information to be substituted for classified information, allowing for the substitution of unclassified information for classified information, or specifically allowing for redaction. Nevertheless, redaction appears to be used as a matter of practice.

8.27 An example of an attempt to use redacted documents can be found in the *Lappas* trial, where 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'.[33]

8.28 The ALRC was informed in one consultation that parties trying to protect information which is the subject of a claim for public interest immunity usually apply to delete or redact that information, rather than rewrite it (for example, by substituting an unclassified summary of the sensitive information) whereas US law specifically allowed the court to supervise the executive in re-writing sensitive information, in addition to permitting sections to be deleted.[34] The Attorney-General's Department submitted that one of the reasons that certain charges in the *Lappas* case had to be dropped was because 'there were no procedures in place allowing for substitution of summaries or stipulation [so that] the documents in question could not be produced in any form.'[35]

8.29 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 ex parte proceedings:

- Section 2712(e)(1) of the US Code[36] provides that, upon the motion of the United States, the court shall stay any action commenced under the section[37] 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 a submission, the plaintiff in a civil action against the

33 *R v Lappas and Dowling* [2001] ACTSC 115, [2]. See also discussion of this case in Ch 7, Ch 8 at [8.101]. [8.166] and [8.229], and Appendix 4.

34 J Renwick, *Consultation*, Sydney, 9 September 2003.

35 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

36 Found in Title 18, Chapter 121.

37 Section 2712(a) of the United States Code allows persons to commence civil actions against the United States for damages for the wilful violation of Ch 119 and Ch 121 of the United States Code, and of specified provisions of the *Foreign Intelligence Surveillance Act 1978* (USA).

Government is given an opportunity to make a submission to the court, not ex parte, and the court may request further information from either party.[38]

- 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.[39]

Methods used in court to present evidence

8.30 In addition to the methods identified at [8.23] above, there are other measures that can be used in open court to impose restrictions on the access to, and disclosure of, classified and security sensitive information that is admitted as evidence in court or tribunal proceedings. These measures include:

- Requiring confidentiality undertakings from lawyers and others who deal with classified or security sensitive material during proceedings, discussed at [8.98] below;

- Using various techniques to hide the identity of a witness or informant, discussed at [8.39] below;

- Requiring the use of security-cleared counsel, discussed in Chapters 6 and 10;

- Using written (rather than oral) questions and answers during otherwise oral testimony or cross-examination, or during the examination or cross-examination of witnesses whose evidence is otherwise on affidavit;[40]

- Having witnesses give evidence in open court which can only be heard through headsets provided to the judge, jury and parties to the proceedings;[41]

---

38 *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.

39 Ibid, s 411 amends (among other sections) s 219 of the *Immigration and Nationality Act* (8 USC s 1189).

40 Australian Federal Police, *Submission CSSI 13*, 18 September 2003. A disadvantage of cross-examination by affidavit is that the element of surprise together with its forensic benefits are lost. A witness could also be required to answer a question put to them in open court by writing a response rather than giving an oral reply: B Leader, *Consultation*, By telephone, 26 August 2003.

41 This technique has been used in the United States for the evidence of witnesses who have been deposed. The video of their testimony is played in open court but with headsets and monitors aimed at the judge and jury. This method also has the benefit of making an impression on the jury in relation to the import-

- Using techniques such as the US 'silent witness rule', under which:

  > the witness would not disclose the information from the classified document in open court. Instead, the witness would have a copy of the classified document before him. The court, counsel and the jury would also have copies of the classified document. The witness would refer to specific places in the document in response to questioning. The jury would then refer to the particular part of the document as the witness answered. By this method, the classified information would not be made public at trial but the defense would be able to present that classified information to the jury.[42]

- Handing up documents in open proceedings that are not to be read in public;[43]

- Admitting material into evidence for particular specified and limited purposes in circumstances where oral cross-examination is not possible;[44]

- Using closed-circuit television or similar technology to protect the identity or location of witnesses or the contents of documents;[45]

- Hearing part of the evidence in the absence of the jury when this does not go to an issue of fact that the jury will have to determine; and

- Establishing appeal mechanisms for any applications for the protection of classified or security sensitive information so that, for example, a party who unsuccessfully applies for an order to close the court to the public or for a suppression order can appeal that order.[46]

8.31 The closure of courts and tribunals to the public and suppression orders are discussed at [8.203] below; the closure of courts and tribunals to a party is discussed in Chapter 9.

---

ance of the information: Federal Bureau of Investigation, *Consultation*, Washington DC, 30 October 2003; Central Intelligence Agency, *Consultation*, Virginia, 24 October 2003.

42 This rule was adopted in *United States v Zettle* 835 F 2d 1059 (4th Cir, 1987), 1063.

43 As in *Andrew v Raeburn* (1874) 9 Ch App 522.

44 Australian Federal Police, *Submission CSSI 13*, 18 September 2003.

45 For example, the head of the British Secret Intelligence Service, Sir Richard Dearlove, 'took the unprecedented step of testifying to the inquiry [into the suicide of David Kelly, the weapons expert]—via audio link to protect his identity—to defend his service': D Evans, 'Awkward Questions Being Asked of MI6 in Wake of Inquiry', *The Canberra Times*, 26 September 2003, 15. Evidence can also be presented on plasma television screens visible only to the judge and jury, and the witness could electronically highlight words in a classified document rather than speak to them: United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003. *Supreme Court Rules 1970* (NSW), Part 36, r 2A allows the court to give directions in relation to the conduct of proceedings, including the giving of evidence, by any audio-visual method or by telephone. However, directions cannot be given under this rule in respect of the evidence given by an accused or which would prevent an accused from attending any part of a proceeding, without the consent of the accused: *Supreme Court Rules 1970* (NSW), Part 75, r 2(8).

46 Australian Federal Police, *Submission CSSI 13*, 18 September 2003. This is discussed at [8.265] below.

8.32 The espionage trial in 2003 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.[47]
>
> 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.[48]

8.33 Section 8 of the *Classified Information Procedures Act* (USA) (CIPA) provides that:

> Writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status.[49]
>
> 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.[50]

8.34 Section 8(c) of CIPA provides that:

> 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

---

47 The ALRC was informed in consultation that one method used to protect evidence was to have special binders for each of the jurors that were to be returned to a court security officer at the end of each day: United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003.

48 *Jury Begins Deliberating in Regan Espionage Case*, Associated Press, <www.sunspot.net/news/nationworld/bal-te.espionage11feb11,0,69298464.story?coll=bal-nationworld-headlines/> at 11 February 2003.

49 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 8(a). This provision recognises that classification is an executive not a judicial function: *Senate Report No 96–823*, United States Congressional and Administrative News, 4294, 4299.

50 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 8(b).

> defendant to provide the court with a proffer of the nature of the information he seeks to elicit.[51]

8.35 The trial of former British MI5 officer David Shayler, who was convicted for breaching the *Official Secrets Act 1989* (UK), provides an interesting example of a regime proposed by the prosecution to protect sensitive evidence as an alternative to in-camera proceedings.[52] The Crown initially made an application under the *Official Secrets Act 1920* (UK), the *Official Secrets Act 1989* (UK) and the Crown Court Rules 1982 (UK)[53] that 'any part of the trial process which touches, or purports to touch, whether directly or indirectly, upon any sensitive operational techniques of the Security and Intelligence Services, and in particular upon their sources of information, including the identity of any officer, contact or agent be held in camera.'[54] The application for the parts of the trial to be heard in camera were supported by two certificates signed by the Home Secretary. One of the certificates contained a Sensitive Schedule, for the benefit of the court, which contained full details about the information for which non-publication was sought and the precise harm that publication would cause. The prosecution invited the trial judge to approve the following regime, designed to avoid the need for an in-camera application to be made, and to conduct as much as possible of the trial in open court:

> 4. (a) the defendant to give notice in writing to the Crown of any matter relating or purporting to relate to security or intelligence which he may seek to raise (whether directly or indirectly); and
>
> (b) if the Crown dispute relevance, that issue to be decided by [the judge] whether on paper or in chambers (pursuant to the Court's inherent powers) so as to avoid any risk of damage;
>
> 5. Obviously all must understand that if the learned judge rules to be relevant (and thus capable of being referred to in open court) a matter which is caught by the terms of the notices then this will inevitably trigger an in camera application.
>
> 6. It should be understood that if this regime is approved, the prosecution in the event of a breach, may apply to the judge to regard that breach as a contempt.
>
> 7. Any such breach will also inevitably lead to the resurrection of the in camera application.[55]

8.36 The judge was satisfied that there was a risk that Shayler might, 'either in the course of cross-examination or in the course of evidence adduced by him or through other witnesses, disclose matters that themselves may cause a risk of damage to nation-

---

51 CIPA is discussed more fully at [8.55]–[8.76] below.

52 In-camera proceedings are discussed below at [8.203] below. *Shayler* is also discussed at [8.46]–[8.48] below.

53 The provisions under these Acts and Rules allowing for closed hearings are set out in the discussion below at [8.203] under the heading 'Closing courts to the public.'

54 *R v Shayler* [2003] EWCA Crim 2218, [10].

55 Ibid, [19].

al security or put any person in danger'.[56] Given the dilemma of identifying in sufficient time when an issue might arise concerning Shayler's intention to raise such matters, the judge accepted the procedure suggested by the Crown. The Court ruled that:

> If the defendant wishes to raise any matter relating or purporting to relate to security or intelligence, he must give the Court advance notice of that, be it raised in the form of questions to any witnesses or once the Crown case has closed, should it be necessary and the case go any further in relation to any evidence he wishes to adduce.[57]

8.37 On appeal, the Court of Criminal Appeal stated that the judge's ruling:

> did not require the applicant to give notice of the questions he proposed to ask, or to provide any proof of evidence of himself or his witnesses. All he had to do was to give notice of any matter relating or purporting to relate to security or intelligence which he wished to raise.[58]

8.38 In the US,[59] an accused in a criminal proceeding must give the court and the prosecution notice if he or she reasonably expects to disclose, or cause the disclosure of, classified information at trial or during any pre-trial proceeding, and must give a description of that classified information. Accordingly, there is a common element of advance notice by the accused of an intention to lead sensitive information in the procedure adopted in *Shayler* in the UK, and the statutory procedure in the US. One difference is that the US procedure applies to all criminal proceedings whereas the procedure used in *Shayler* appears to have eventuated as part of a case-by-case handling of the issue by the courts and the parties involved. For the reasons discussed in Chapter 10, the ALRC believes that there is merit in having in place a mechanism which both requires pre-trial disclosure by all parties of an intention to lead or cause the disclosure of classified or security sensitive information at trial, and gives the court flexibility to deal with unexpected disclosures of classified information during testimony at trial.

Methods used in court to protect sources of information

8.39 In cases involving classified or security sensitive information, including terrorism cases, intelligence services may wish to protect the identity of an informant, the identity of agents or other details of their operations.[60] Some methods used to protect identity, such as the use of in-camera hearings and suppression orders, are also routine-

---

56 Ibid, [21].
57 Ibid, [21].
58 Ibid, [21].
59 Discussed at [8.55]–[8.76] below.
60 In other cases, an individual's occupation may need to be kept secret in court proceedings: B Leader, *Consultation*, By telephone, 26 August 2003. An example of such cases were family law disputes relating to residence and contact issues where the occupation of one party to the dispute as an ASIS officer had to be kept secret. These cases were heard in closed court, transcript was prepared on special coloured paper and confidentiality undertakings were obtained: Advisory Committee member, *Consultation*, Melbourne, 29 August 2003.

ly used to protect other forms of sensitive information. In-camera hearings and suppression orders are discussed at [8.203] below.

8.40 Other mechanisms to protect the identity of a witness or informant include: referring to the witness or informant by letter or number only (for example, Witness 'X'); orders suppressing the person's identity; the use of a mask or voice distorter;[61] 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.[62] This last method was used in the committal proceeding in 1994 of George Sadil in the ACT Magistrates Court for several espionage and official secrets offences under the *Crimes Act 1914* (Cth).[63]

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

> If the real identity of an approved officer or approved person[64] who is or was covered by an authorisation,[65] 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.[66]

8.42 The *Administrative Appeals Tribunal Act 1975* (Cth) provides that, 'if the Director-General of Security so requests, the AAT 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'.[67]

---

61 E Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, 558.

62 I Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113, 118.

63 Commonwealth Director of Public Prosecutions, *Consultation*, By telephone, 3 November 2003. However, the Commonwealth DPP expressed the view that this was an exceptional order and that such an order would have been more difficult to obtain at a trial before a jury.

64 'Approved officer' and 'approved person' are defined in *Crimes Act 1914* (Cth), s 15XA.

65 'Authorisation' is defined in s 15XA as an authorisation that is in force under s 15XG or 15XH of the Act.

66 *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.

67 *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(11). See also *Law Enforcement (Controlled Operations) Act 1997* (NSW), s 28 which provides for the protection of the identity of participants in authorised operations (as defined in s 3). For example, a court, tribunal, Royal Commission or other commission of inquiry may allow a participant in an authorised operation who has been authorised to participate in that operation under an assumed name to appear before it under that name. The *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW), s 14(1) and (2)(a) allows a court, tribunal, Royal Commission or other commission of enquiry to order that 'an officer in respect of whom an assumed identity approval is or was in force is in issue or may be disclosed' to appear before it under a code number or a code name.

8.43 The *Evidence Act 1977* (Qld) provides for a covert operative[68] to give evidence anonymously in a proceeding before a court, including criminal proceedings, where that evidence was obtained when the operative was engaged in activities for a controlled operation.[69] The chief executive officer of a law enforcement agency may issue a witness anonymity certificate for the purposes of a proceeding if he or she thinks that it is reasonably necessary to protect a former or present covert operative of the agency who is, or may be, required to give evidence.[70] A senior police officer may also issue a witness anonymity certificate if he or she thinks that it is reasonably necessary to protect a former or present covert operative for the police service.[71] The Act sets out a number of matters that the certificate must state, including the name the witness used in the covert operation; that the witness has not been convicted of any offence other than a stated offence; if the witness is a police officer whether he or she has been found guilty of specified types of misconduct or breach of discipline; and any adverse comments about the credibility of the witness made by a court of which the person making the certificate is aware.[72]

8.44 When a witness anonymity certificate is filed, the protected witness may give evidence in the proceeding under the name he or she used in the controlled operation.[73] A copy of the certificate must be given to the accused or his or lawyer in the case of criminal proceedings, and to each other party in the proceeding or their lawyer in the case of civil proceedings.[74] The court or entity before which the proceeding is conducted is empowered to make any order it considers necessary to protect the identity of the protected witness. These orders include an order prohibiting sketching of the witness and an order that the witness give evidence in the absence of the public.[75] However, a party may apply to the court for leave to ask questions of a witness, including a protected witness, that if answered may disclose the protected witness's identity or address.[76] The court may direct that the application be heard in the absence of the empanelled jury and of the public.[77] The court can only grant leave if it is satisfied that:

> (a) there is some evidence that, if believed, would call into question the credibility of the protected witness; and

---

68 'Covert operative' for a controlled operation conducted by a law enforcement agency, means a police officer or another person named as a covert operative in an approval under the *Police Powers and Responsibilities Act 2000* (Qld), s 178: *Evidence Act 1977* (Qld), s 21B. 'Law enforcement agency' is defined as the police service or the Crime and Misconduct Commission.

69 'Controlled operation' means 'a controlled operation approved under the *Police Powers and Responsibilities Act 2000* (Qld), ch 5, Pt 2, Div 3 for the purposes of an investigation being conducted by a law enforcement agency': *Evidence Act 1977* (Qld), s 21B.

70 *Evidence Act 1977* (Qld), s 21D(1).

71 Ibid, s 21D(2). A 'senior police officer' means a person performing functions in the police service as a deputy commissioner or the assistant commissioner responsible for crime operations: *Evidence Act 1977* (Qld), s 21D(7).

72 See *Evidence Act 1977* (Qld), s 21E.

73 Ibid, s 21F.

74 See Ibid, s 21G.

75 Ibid, s 21H.

76 Ibid, s 21I(1).

77 Ibid, s 21I(2).

> (b) it is in the interests of justice for the relevant party to be able to test the credibility of the protected witness; and
>
> (c) it would be impractical to test properly the credibility of the protected witness without knowing the actual identity of the witness.[78]

8.45 The *Evidence Act 1977* (Qld) also provides that the chairperson of the Crime and Misconduct Commission must review the giving of each witness anonymity certificate filed by the police service as soon as practicable after the end of the proceeding to which the certificate relates, and in any case within three months after the end of the year in which the certificate was filed.[79] The chairperson must consider whether it was appropriate to give the certificate.[80] If the chairperson considers that it was inappropriate, he or she must notify the accused person or their lawyer in the case of criminal proceedings, and each party to the proceeding in the case of civil proceedings.[81] The ALRC notes that these procedures take place *after* the completion of the proceedings. From the perspective of affording fairness to an accused, it seems preferable that, whenever a witness anonymity certificate is issued or a witness is otherwise allowed to give evidence anonymously, a review of whether such a course of action is warranted should be undertaken by an independent person prior to the informant giving evidence.

8.46 The trial of former MI5 officer David Shayler provides examples of methods used to protect the identity of sources of information.[82] The prosecution proposed that three serving MI5 members and one former member should give evidence from behind a closed screen without being named.

> The judge accepted … [the] submission that he must take into account the prejudice likely to arise by reason of the 'aura' that anonymity would cast on the evidence in the case. The judge also considered whether the evidence to be given by each witness was sufficiently relevant and important to make it unfair to the prosecution to proceed without it; the extent to which the creditworthiness of each witness had been properly investigated by the Crown, and the results of that investigation disclosed, and the need to balance the need for protection to the necessary extent against any unfairness or appearance of unfairness in the instant case. …
>
> [The judge found] that because of the importance of the witnesses to the prosecution case were he not to make the order sought preserving their anonymity, the prosecution would be faced with a stark choice: either to call the witnesses and expose them to the risk, or abandon the case. … As to the possible prejudice to the defendant, he knew the names of the witnesses, and having regard to the nature of their trial their anonymity would not give rise to any real risk of prejudice against him.[83]

8.47 Accordingly, the four past and present MI5 officers, referred to as Messrs A, B, C and D, gave evidence anonymously.

---

78 Ibid, s 21I(3).
79 Ibid, s 21J(3)(a).
80 Ibid, s 21J(3)(b).
81 See Ibid, s 21J(3)(c).
82 Also discussed at [8.35]–[8.38] above.
83 *R v Shayler* [2003] EWCA Crim 2218, [14] and [15].

> Brown paper and bits of sticky tape were used to hide the identity of an MI5 agent …
>
> The judge, Mr Justice Moses, told the jury the man would be referred to as witness B and people in the public gallery would not be able to see him. …
>
> The jury, Mr Shayler, lawyers, court staff and jurors were the only ones not shielded from the witness box …
>
> Members of the public sat behind large brown screens placed in front of the gallery above the court. The press sat at the back of the court with an usher. Representatives could only hear Mr B give evidence.[84]

8.48 Files marked 'Top Secret' were shown to the jury. Names of agents had been blacked out to protect their identities and jurors were told not to disclose the contents.[85]

8.49 The Canadian Criminal Code contains a provision allowing the court in certain cases, including cases where the accused has been charged with a terrorism offence, to order that any witness testify:

> (a) outside the court room, if the judge or justice is of the opinion that the order is necessary to protect the safety of the witness; and
>
> (b) outside the court room or behind a screen or other device that would allow the witness not to see the accused, if the judge or justice is of the opinion that the order is necessary to obtain a full and candid account from the witness.[86]

8.50 Where testimony is to be outside the courtroom, arrangements are to be made for 'the accused, the judge or justice and the jury to watch the testimony of the complainant or witness by means of closed-circuit television or otherwise and the accused is permitted to communicate with counsel while watching the testimony.'[87]

8.51 Although these Canadian provisions are not aimed specifically at the protection of classified and security sensitive information, they demonstrate a statutory recognition of mechanisms—the giving of evidence behind a screen or outside court with the assistance of closed circuit television—which can be used to protect the identities of informants.

8.52 German courts use a different 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 written statements made by them and the in-court testimony of the police officers who interrogated them in place of oral evi-

---

84 *Shayler Trial Calls Secret MI5 Witness*, <www.guardian.co.uk/shayler/article/0,2763,822681,00.html> at 30 October 2002.

85 *Secret Files Shown at Shayler Trial*, BBC News, <http://news.bbc.co.uk/1/hi/uk/2372083.stm> at 29 October 2002.

86 See *Criminal Code* [RS 1985, c C–46] (Canada), s 486(2.101) and (2.102).

87 Ibid.

dence given in open court. 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.[88]

> 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.[89]

8.53 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.[90]

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.[91]

---

88 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.

89 H Reiter, 'Hearsay Evidence and Criminal Process in Germany and Australia' (1984) 10 *Monash University Law Review* 51, 69–70.

90 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.

91 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.

8.54 There are, of course, differences between the German and Australian systems. Among other things, 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.[92] The risks of hearsay evidence include a danger that the repetition will be inaccurate and the potential for the fabrication of evidence. Some of the dangers associated with the use of hearsay evidence are discussed in Chapter 9 at [9.8].

International models

United States

8.55 CIPA addresses—but does not entirely solve—the greymail issue by providing a procedural framework for the disclosure and admission of classified information in criminal trials and requiring pre-trial court rulings on the admissibility of such evidence.[93] CIPA 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.[94]

8.56 CIPA provides that at any time following the filing of the indictment or information, any party may move for a pre-trial conference to consider matters relating to classified information that may arise in the prosecution.[95] Following such a motion, or on its own motion, the court is to hold a pre-trial conference at which, among other things, it is to set down a timetable for discovery and the provision of notice required by s 5 of the Act (see [8.60] below) and consider 'any matters which relate to classified information or which may promote a fair and expeditious trial'.[96] However, no substantive issues about the use of classified information are to be decided at the pre-trial conference.[97] These issues are to be determined at a pre-trial hearing held pursuant to s 6 of the Act.[98]

8.57 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'. The terms of a protective order may include, but are not limited to, provisions:

> (1) prohibiting the disclosure of the information except as authorized by the court; (2) requiring storage of material in a manner appropriate for the level of classification assigned to the documents to be disclosed; (3) requiring controlled access to the material during normal business hours and at other times upon reasonable notice; (4) requi-

92 See International Covenant on Civil and Political Rights, Art 14(3)(e) set out in Ch 7 and Appendix 3.
93 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA).
94 See *United States v Baptista-Rodriguez*, 17 F 3d 1354, 1363 (11th Cir, 1994).
95 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 2.
96 Ibid, s 2. In order to encourage open discussions at pre-trial conferences, the section also provides that no admission made by the defendant or his or her lawyer at the pre-trial conference can be used against the defendant unless the admission is in writing and signed by both the defendant and his or her lawyer.
97 *Senate Report No 96–823*, United States Congressional and Administrative News, 4294, 4298–4299.
98 See [8.62] below.

> ring the maintenance of logs recording access by all persons authorized by the court to have access to the classified information in connection with the preparation of the defense; (5) requiring the making and handling of notes taken from material containing classified information; and (6) authorizing the assignment of government security personnel and the provision of Government storage facilities.[99]

8.58 Under s 4, upon 'sufficient showing' the court may 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.

8.59 The Government may demonstrate that the use of these alternatives is necessary in an in-camera and ex parte submission to the court.[100] The US Criminal Resources Manual states:

> Where supported by law, the prosecutor during the proceedings, should strive to have the court exclude as much classified information as possible from the government's discovery obligation. Second, to the extent that the court rules that certain material is discoverable, the prosecutor should seek the court's approval to utilize the alternative measures described in section 4, ie unclassified summaries and/or stipulations. The court's denial of such a request is subject to interlocutory appeal.[101]

8.60 Following discovery under s 4, there are three critical pre-trial stages in the handling of classified information under CIPA.[102] Firstly, the defendant must notify the Government and the court in writing if he or she reasonably expects to disclose classified information at the trial or in pre-trial proceedings. The notice must specify in detail the classified information which the defendant intends to rely upon. The notification is to be given 'within the time specified by the court or, where no time is specified, within thirty days prior to trial'.[103] 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.[104] The notice requirements, do not, however, vio-

---

99 *Senate Report No 96–823*, United States Congressional and Administrative News, 4294, 4299.

100 *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.

101 Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam>, 2054, Synopsis of the Classified Information Procedure Act (CIPA).

102 Ibid, 2054, Synopsis of Classified Information Procedures Act.

103 *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.

104 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 5(b).

late the defendant's rights against self-incrimination.[105] In *United States v Poindexter*, the court stated:

> [T]here is no compulsion on the defendant to reveal when he will testify or even whether he will testify. All he is required to do under CIPA is to identify the classified information on which his side intends to rely in the course of its overall presentation, not who will disclose it as a part of any particular testimony.[106]

8.61 In *United States v Collins*, the Court of Appeal for the 11th Circuit stated:

> The Section 5(a) notice is the central document in CIPA. After the CIPA procedures have been followed, the government should not be surprised at any criminal trial when the defense discloses or causes to be disclosed, any item of classified information. … The court must not countenance a Section 5(a) notice which allows a defendant to cloak his intentions and leave the government subject to surprise at what may be revealed in the defense. To do so would merely require the defendant to reduce 'greymail' to writing.[107]

8.62 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.[108] Prior to this hearing, the Government must provide the defendant with notice of the specific classified information in issue.[109] 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.[110]

8.63 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.[111] Any hearing on a motion in this regard must be held in camera at the request of the Attorney General.[112] The court is required to grant such a motion if it finds that the statement or

---

105 *United States v Wen Ho Lee* 90 F Supp 2d 1324 (DNM, 2000), 1324; *United States v Poindexter* 725 F Supp 13 (DDC, 1989), 31; *United States v Jolliff* 548 F Supp 227 (DMd, 1981), 231.

106 *United States v Poindexter* 725 F Supp 13 (DDC, 1989), 33.

107 *United States v Collins* 720 F 2d 1195 (11th Cir, 1983), 1199–1200.

108 The courts have emphasised that relevance and admissibility are separate issues to be determined. Not every document that is relevant will necessarily be admissible; for example the application of government privilege may render the document inadmissible: see *United States of America, Appellant v Richard Craig Smith, Appellee* 780 F 2d 1102 (US Court of Appeals for the 4th Circuit, 1985).

109 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), 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).

110 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(a). Any portion of any such hearing shall also be held in camera if the Attorney General certifies to the court that a public proceeding may result in the disclosure of classified information.

111 Ibid, s 6(c). It seems that the court's determination concerning substitutions and summaries is to be made following a hearing that is separate from the hearing in relation to relevance and admissibility.

112 Ibid, s 6(2)(c).

summary 'will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information'.[113] The court must set out in writing the basis for its determination in relation to each item of classified information.[114] 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'.[115] 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.[116]

8.64 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.[117]

8.65 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.[118]

8.66 Section 10 of CIPA provides that:

> In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.

---

113 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).

114 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(a).

115 Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam> 2054, Synopsis of Classified Information Procedures Act.

116 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(f).

117 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).

118 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>.

8.67 All in-camera proceedings and hearings held pursuant to CIPA are sealed and preserved for the appellate record.[119] Thus, if a court rules that classified information may not be used, the records of any in-camera hearings held under the Act to determine admissibility must be sealed and preserved for use in the event of an appeal.

8.68 At the time of writing, the trial date of Zacarias Moussaoui, the alleged conspirator in the attacks on the World Trade Centre and Pentagon on 11 September 2001, had been indefinitely adjourned.[120] 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 Department of Justice:

> 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.[121]

8.69 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.[122] In April 2003, the 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'.[123] The Justice Department said that it should be allowed to edit some of the documents before they were made public.[124]

8.70 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.[125] A number of newspapers had applied for the release of the transcripts.

---

119 *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.

120 The case of Zacarias Moussaoui is discussed in Ch 7.

121 J Markon, *US Files Terror Briefs in Secrecy*, Washington Post, <www.washingtonpost.com/ac2/wp-dyn/A27772-2003Mar13.html> at 27 March 2003.

122 The text of the First Amendment to the US Constitution is set out in Appendix 3.

123 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> at 21 April 2003.

124 Ibid.

125 D Russakoff, 'NJ Judge Unseals Transcript In Controversial Terror Case', *The Washington Post*, 25 June 2003, A03.

Court security officer

8.71 Section 9 of CIPA provides in part, that:

> [T]he Chief Justice of the United States, in consultation with the Attorney General, the Director of Central Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court.

8.72 Security procedures established by the Chief Justice provide for the appointment of a court security officer in any proceeding in a criminal case or related appeal where classified information is within, or expected to be within, the custody of the court.

> The Attorney General or the Department of Justice Security Officer, with the concurrence of the head of the agency or agencies from which the classified information originates, or their representatives, shall recommend to the court persons qualified to serve as court security officer. The court security officer shall be selected from among those persons recommended.
>
> The court security officer shall be an individual with demonstrated competence in security matters, and shall, prior to designation, have been certified to the court in writing by the Department of Justice Security Officer as cleared for the level and category of classified information that will be involved. The court security officer may be an employee of the Executive Branch of the Government detailed to the court for this purpose. One or more alternate court security officers, who have been recommended and cleared in the manner specified above, may be designated by the court as required.
>
> The court security officer shall be responsible to the court for document, physical, personnel and communications security, and shall take measures reasonably necessary to fulfil these responsibilities. The court officer shall notify the court and the Department of Justice Security Officer of any actual, attempted or potential violation of security procedures.[126]

8.73 The security procedures also provide that any in-camera proceeding, including a pre-trial conference, motion hearing or appellate hearing, concerning the use, relevance or admissibility of classified information must be heard in secure quarters recommended by the court security officer and approved by the court.[127] The secure quarters are to be located within the Federal courthouse:

> unless it is determined that none of the quarters available in the courthouse meets, or can reasonably be made equivalent to, security requirements of the Executive Branch applicable to the level and category of classified information involved. In that event, the court shall designate the facilities of another United States Government agency,

---

126 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, s 2.

127 For example, the United States District Court for the Eastern District of Virginia has specially built facilities for the storage of classified information: Federal Bureau of Investigation, *Consultation*, Washington DC, 30 October 2003.

> recommended by the court security officer, which is located within the vicinity of the courthouse, as the site of the proceedings.[128]

8.74 The court security officer must arrange for the installation of security devices and take any other measures necessary to protect against unauthorised access to classified information. The court security officer must certify in writing to the court that the quarters are secure prior to any hearing or other proceeding.[129] The court security officer is responsible for the safekeeping of all classified information submitted to the court. Classified information, when not in use, is to be stored by the court security officer in a container meeting the requisite security standards.[130] The security procedures apply to all 'papers, documents, motions, pleadings, briefs, notes, records of statements involving classified information, notes relating to classified information taken during in camera proceedings, orders, affidavits, transcripts, untranscribed notes of court reporter, magnetic recordings or any other submissions or records which contain classified information'.[131] Unless authorised by a protective order, the defendant's lawyers are not allowed custody of classified information provided by the Government. The court, in its discretion, may allow the defendant's lawyers access to the classified information provided by the Government in secure quarters which have been approved, but the classified information remains in the control of the court security officer.[132]

8.75 The court security officer, after consultation with the Government, is responsible for marking all court documents containing classified information with the appropriate level of classification and any special access controls. Every document filed by the defendant in the case is to be filed under seal and promptly released to the court security officer, who must examine it and, in consultation with the attorney for the Government or representative of the appropriate agency, determine whether it contains classified information. Where a determination is made that the document contains classified information, the court security officer must ensure that the document is marked with the appropriate classification marking. If it is determined that the document does not contain any classified information, the document is to be unsealed and placed on the public record.[133] The court security officer is also responsible 'for the establishment and maintenance of a control and accountability system for all classified information received by or transmitted from the court.'[134]

8.76 There are a number of features of CIPA which the ALRC has adapted in making its Proposals. See the further discussion of CIPA in Chapter 10 and, for example, Proposals 10–5, 10–10, 10–13 and 10–36.

---

128 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, s 3.
129 Ibid, s 3.
130 Ibid, s 7(b).
131 Ibid, s 7(a).
132 Ibid, s 8(a).
133 Ibid, s 9(a).
134 Ibid, s 9(b).

United Kingdom

8.77 Unlike the US, the UK does not have a statute dealing specifically with the disclosure and treatment of classified information. Rather, it has a statute dealing with the disclosure of evidence generally. The *Criminal Procedure and Investigations Act 1996* (UK) deals with the disclosure of evidence in certain proceedings[135] and investigations.[136] In general terms, the regime for disclosure entails the following steps:

(a) The prosecution makes primary disclosure to the defence of material which, in the prosecutor's opinion, might undermine the case against the accused.[137] However, material must not be disclosed 'to the extent that the court, on an application by the prosecutor, concludes it is not in the public interest to disclose it and orders accordingly'.[138]

(b) The defence, as a consequence of primary disclosure, must give a defence statement to the prosecutor and the court[139] which sets out in general terms the nature of his or her defence, indicates the matters in issue with the prosecution and, in relation to each such matter, the reason why he or she takes issue with the prosecution.[140]

(c) The prosecution makes secondary disclosure of material which might reasonably be expected to assist the accused's defence as disclosed by the defence statement,[141] although material must not be disclosed 'to the extent that the court, on an application by the prosecutor, concludes it is not in the public interest to disclose it and orders accordingly'.[142]

(d) If the accused has reasonable cause to believe that there is prosecution material which might reasonably be expected to assist the defence as disclosed by the defence statement that has not been disclosed to the accused, the accused may apply for an order requiring disclosure of that material by the prosecution.[143] However, material must not be disclosed 'to the extent that the court, on an

---

135 See *Criminal Procedure and Investigations Act 1996* (UK), s 1. For example, the disclosure provisions apply where a person is charged with a summary offence in respect of which a court proceeds to summary trial and in respect of which he or she pleads not guilty or where a person is charged with an indictable offence in respect of which he or she is committed for trial: *Criminal Procedure and Investigations Act 1996* (UK), s 1(1)(a) and 1(2)(a).

136 The disclosure regime applies to all offences into which a criminal investigation was commenced on or after 1 April 1997: S Farrell, *Changes in the Law of Disclosure: The New Disclosure Scheme Under the Criminal Procedure and Investigation Act 1996*, <www.2gardenct.law.co.uk/Chambers%20News/Seminars/Resources/Crime%202%20-%205FA's%20Paper.pdf> at 26 November 1998.

137 See *Criminal Procedure and Investigations Act 1996* (UK), s 3.

138 Ibid, s 3(6).

139 Ibid, s 5.

140 Ibid, s 6.

141 Ibid, s 7.

142 Ibid, s 7(5).

143 Ibid, s 8(2).

> application by the prosecutor, concludes it is not in the public interest to disclose it and orders accordingly'.[144]

8.78 In a summary proceedings, where a court has ordered that material not be disclosed in the public interest,[145] the accused may, before he or she is convicted, acquitted or the prosecutor decides not to proceed with the case, apply for a review of the question of whether it is still not in the public interest to disclose material affected by its order.[146] In other cases where the court has ordered that material not be disclosed in the public interest, the court must keep under review, without the need for an application, the question whether at any given time it is still not in the public interest to disclose material affected by its order.[147] These provisions appear well suited to accommodate a situation where sensitive material loses its sensitivity some time after the court's original order in relation to disclosure. Accordingly, the ALRC has adopted this feature of the UK Act in making its Proposals. See Proposal 10–28.

8.79 The Act imposes upon the accused a duty of confidentiality in relation to objects or information obtained as a result of the statutory disclosure regime. The accused must not use or disclose those objects or that information except as provided for in the Act.[148] For example, the accused may use or disclose the object or information 'in connection with the proceedings for whose purpose he was given the object or allowed to inspect it'[149] or may use or disclose information 'to the extent that it has been communicated to the public in open court'.[150] The Act provides that:

> It is a contempt of court for a person knowingly to use or disclose an object or information recorded in it if the use or disclosure is in contravention of section 17.[151]

8.80 The Act mandates the Secretary of State to prepare a code of practice covering, among other things, the disclosure of information.[152] The Act provides that:

> The code may provide that if the person required to reveal material has possession of material which he believes is sensitive[153] he must give a document which—
>
> (a) indicates the nature of that material, and
>
> (b) states that he so believes.[154]

---

144 Ibid, s 8(5). A court can also make such an order under s 9(8) exempting material from the prosecution's continuing duty of disclosure on the ground of public interest.

145 Being orders made pursuant to Ibid, s 3(6), 7(5), 8(5) or 9(8).

146 Ibid, s 14(2). The court must review that question and, if it concludes that it is in the public interest to disclose material to any extent, it shall order accordingly: s 14(3).

147 Ibid, s 15(3) and 15(4). Note that the accused may still apply to the court for such a review. If the court at any time concludes that it is in the public interest to disclose material to any extent, it shall order accordingly: s 15(5).

148 Ibid, s 17(1).

149 Ibid, s 17(2)(a).

150 Unless the proceedings are to deal with a contempt of court under s 18. See Ibid, s 17(3)(b).

151 Ibid, s 18(1).

152 See Ibid, s 23.

153 Material is 'sensitive to the extent that its disclosure under Part 1 [of the Act] would be contrary to the public interest': Ibid, s 24(8).

8.81 A Code of Practice has been issued under the *Criminal Procedure and Investigations Act 1996*, which applies in England and Wales. The Code delineates the functions of the investigator, the officer in charge of the investigation, and the disclosure officer. The 'disclosure officer' is defined as:

> the person responsible for examining material retained by the police during the examination, revealing material to the prosecutor during the investigation and any criminal proceedings resulting from it, and certifying that he has done this; and disclosing material to the accused at the request of the prosecutor.[155]

8.82 The Code of Practice provides that any material which is believed to be sensitive[156] must be either listed on a schedule of sensitive material or, in exceptional cases, revealed to the prosecutor separately.[157] Other than in exceptional circumstances,[158] the Code provides that:

> the disclosure officer is to list on a sensitive schedule any material which he or she believes it is not in the public interest to disclose, and the reason for that belief. The schedule must include a statement that the disclosure officer believes the material to be sensitive. Depending on the circumstances, examples of such material may include among others:
>
> - material relating to national security;
> - material received from the intelligence and security agencies;
> - material relating to intelligence from foreign sources which reveals sensitive intelligence gathering methods; … [159]

8.83 In exceptional circumstances, the investigator must reveal the existence of the material to the prosecutor separately.[160] Exceptional circumstances include where an investigator considers that material is so sensitive that its revelation to the prosecutor by means of an entry on the sensitive schedule is inappropriate. This applies 'where compromising the material would be likely to lead directly to the loss of life or directly

---

154 Ibid, s 24(2).

155 *Code of Practice Issued under Part II of the Criminal Procedure and Investigations Act 1996 (UK)*, 1 April 1997, [2.1]. The Code provides that 'an investigator is any police officer involved in the conduct of a criminal investigation. All investigators have a responsibility for carrying out the duties imposed on them under this code, including in particular recording information, and retaining records of information and other material in the investigation': *Code of Practice Issued under Part II of the Criminal Procedure and Investigations Act 1996 (UK)*, 1 April 1997, [2.1].

156 'Sensitive material' is defined as 'material which the disclosure officer believes, after consulting with the officer in charge of the investigation, it is not in the public interest to disclose': *Code of Practice Issued under Part II of the Criminal Procedure and Investigations Act 1996 (UK)*, 1 April 1997, [2.1].

157 Ibid, [6.4].

158 As provided for in paragraph 6.13 of the Code of Practice.

159 *Code of Practice Issued under Part II of the Criminal Procedure and Investigations Act 1996 (UK)*, 1 April 1997, [6.12].

160 This is similar to the position in Australia as set out in Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/prosecutions/disclosure/> F8. See discussion on guidelines at [8.272] below.

threaten national security.'[161] The investigator must ensure that the prosecutor is able to inspect the material so that he or she can ascertain whether a court needs to rule on its disclosure.[162] The disclosure officer can prevent the prosecutor from taking a copy of the material if he or she believes it is too sensitive to be copied.[163]

8.84 The Code of Practice also deals with the disclosure of sensitive material to the accused:

> If a court concludes that it is in the public interest that an item of sensitive material must be disclosed to the accused, it will be necessary to disclose the material if the case is to proceed. This does not mean that sensitive documents must always be disclosed in their original form: for example, **the court may agree** that sensitive details still requiring protection should be blocked out, or that documents may be summarised, or that the prosecutor may make an admission about the substance of the material under section 10 of the *Criminal Justice Act 1967*.[164] [emphasis added]

8.85 The element of court approval for any summary or admission in lieu of full disclosure is a feature of both the models in the US and the UK, which the ALRC has adapted in making its Proposals. However, in this regard, the model in the United States is more comprehensive. See Proposal 10–10(b)(i)–(iii).

Canada

8.86 The *Anti-Terrorism Act 2001* (Canada) amended, among other Acts, the *Canada Evidence Act*[165] to protect certain information from disclosure during proceedings.[166] Unlike US and UK models described above, which apply exclusively to criminal proceedings, the Canadian provisions apply to both criminal and civil proceedings. The ALRC has adopted a similar approach in making the Proposals in this Discussion Paper.[167] The *Canada Evidence Act* provides that:

> Subject to section 38 to 38.16, a Minister of the Crown in right of Canada or other official may object to the disclosure of information before a court, person or body with jurisdiction to compel the production of information by certifying orally or in

---

161 *Code of Practice Issued under Part II of the Criminal Procedure and Investigations Act 1996 (UK)*, 1 April 1997, [6.13].

162 Ibid, [6.14].

163 Ibid, [7.4].

164 Ibid, [10.5]. *Criminal Justice Act 1967* (UK), s 10(1) provides that 'Subject to the provisions of this section, any fact of which oral evidence may be given in any criminal proceedings may be admitted for the purpose of those proceedings by or on behalf of the prosecutor or defendant, and the admission by any party of any such fact under this section shall as against that party be conclusive evidence in those proceedings of the fact admitted.' Note that the Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/prosecutions/disclosure/> does not canvass alternatives to full disclosure of sensitive material to an accused. See discussion at [8.274]–[8.276] below.

165 [RS 1985, c C-5].

166 The provisions in the Act protecting disclosure of information are in Part I, which 'applies to all criminal proceedings and to all civil proceedings and other matters whatever respecting which Parliament has jurisdiction': *Canada Evidence Act* [RS 1985, c C–5], s 2.

167 See discussion in Ch 10 and Proposals 10–1, 10–4 and 10–7.

> writing … that the information should not be disclosed on the grounds of a specified public interest.[168]

8.87 The court may order disclosure of the information if it determines that this disclosure would not encroach upon a specified public interest.[169] If the court considers that disclosure of the information would encroach upon a specified public interest, but that the public interest in disclosure outweighs the specified public interest, the court may authorise disclosure of all the information or disclosure in a way that is most likely to limit any encroachment upon the specified public interest. Examples of the latter approach would include disclosure of a part or summary of the information, or a written admission of facts relating to the information.[170] The Canadian model, in common with the US and UK models, requires court authorisation or approval of alternative methods of disclosure to full disclosure. If the court does not authorise disclosure, it must by order prohibit disclosure of the information.[171]

8.88 Hearings to determine objections and appeals in relation to court orders authorising disclosure of information are to be heard in private[172] and the court may give any person an opportunity to make representations ex parte.[173]

8.89 The Act establishes a regime for the notification to the Attorney General of the expected disclosure of 'potentially injurious information'[174] and 'sensitive information'[175] during proceedings:[176]

> (1) Every participant who, in connection with a proceeding is required to disclose, or expects to disclose or cause the disclosure of, information that the participant believes is sensitive information or potentially injurious information shall, as soon as possible, notify the Attorney General of Canada in writing of the possibility of the disclosure, and of the nature, date and place of the proceeding.[177]
>
> (2) Every participant who believes that sensitive information or potentially injurious information is about to be disclosed, whether by the participant or another person, in the course of a proceeding shall raise the matter with the person presiding at the proceeding and notify the Attorney General of Canada in writing of the matter as soon as possible, whether or not notice has been given under sub-

---

168 *Canada Evidence Act* [RS 1985, c C–5], s 37(1).
169 Ibid, s 37(4.1).
170 Ibid, s 37(5). See also discussion on public interest immunity at [8.118] below.
171 Ibid, s 37(6).
172 Ibid, s 37.21(1).
173 Ibid, s 37.21(2)(b).
174 'Potentially injurious information' means 'information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security': Ibid, s 38.
175 'Sensitive information' means 'information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard': Ibid, s 38.
176 'Proceeding' means a 'proceeding before a court, person or body with jurisdiction to compel the production of information': Ibid, s 38.
177 'Participant' means a 'person, who, in connection with a proceeding, is required to disclose, or expects to disclose, or cause the disclosure of, information': Ibid, s 38.

> section (1). In such circumstances, the person presiding shall ensure that the information is not disclosed other than in accordance with this Act.[178]

8.90 Information notified to the Attorney General pursuant to these provisions must generally not be disclosed in connection with a proceeding.[179] The Attorney General may apply to the Federal Court for an order with respect to the disclosure of information about which notice was given under these sections.[180] The judge must hear the Attorney General's representations in relation to the identity of all parties or witnesses who may be affected by either the prohibition of disclosure or the conditions upon which disclosure is subject, and concerning persons who should be given notice of any hearing in the matter.[181] The judge must also decide whether it is necessary to hold any hearing of the matter.[182] The judge may order the disclosure of the information unless he or she believes that such disclosure would be injurious to international relations, national defence or national security.[183] Alternatively, the judge may authorise disclosure in a way most likely to limit any injury to international relations, national defence or security that may arise from disclosure by imposing conditions on disclosure or authorising the disclosure in full or in part of the information, a summary of the information or a written admission of facts relating to the information.[184] If the judge does not authorise disclosure of the information, whether in full, in part or subject to conditions, he or she must, by order, confirm the prohibition of disclosure.[185] The judge conducting a hearing of the matter, and a court hearing an appeal or review of a disclosure order or prohibition of disclosure order made by the judge, are empowered to 'make any order that the judge or court considers appropriate in the circumstances to protect the confidentiality of the information to which the hearing, appeal or review relates'.[186] Further, the court records relating to the hearing, appeal or review are confidential, and the judge or court may order that they be sealed and kept in a location to which the public has no access.[187]

---

178 Ibid, s 38.01(1) and (2). Certain exceptions are stipulated in relation to the obligation to give notice, including where the information is disclosed by a person in connection with a proceeding, if the information is relevant to that proceeding: see s 38.01(6) and (7).

179 Ibid, s 38.02(1). Note that the Attorney General may authorise the disclosure of the information, in part or in full, subject to any conditions he or she considers appropriate: *Canada Evidence Act* [RS 1985, c C–5], s 38.03(1). Provision is also made for the Attorney General to enter into a disclosure agreement permitting full or partial disclosure of the information subject to conditions: see s 38.04(6).

180 Application may also be made in respect of expected disclosures of information during a proceeding notified to the Attorney General by an official, other than a participant: see *Canada Evidence Act* [RS 1985, c C–5], s 38.01(3) and (4), and 38.04(1).

181 Ibid, s 38.04(5)(a).

182 Ibid, s 38.04(5)(b).

183 Ibid, s 38.06(1).

184 Ibid, s 38.06(2).

185 Ibid, s 38.06(3). An order made under s 38.06(1)–(3) may be appealed to the Federal Court of Appeal. The appeal is to be brought within 10 days after the day on which the order is made or within any further times that the court considers appropriate: *Canada Evidence Act* [RS 1985, c C–5], s 38.09. A court hearing an appeal or a review of an order made under s 38.06(1)–(3) must give the Attorney General the opportunity to make representations ex parte: *Canada Evidence Act* [RS 1985, c C–5], s 38.11(2).

186 *Canada Evidence Act* [RS 1985, c C–5], s 38.12(1).

187 Ibid, s 38.12(2).

8.91 If a court makes an order resulting in the disclosure of information, the Attorney General may issue a certificate that prohibits such disclosure for the purpose of protecting, among other things, national defence or national security.[188] The effect of the certificate is that, notwithstanding any other provision in the Act, disclosure of the information is prohibited in accordance with the terms of the certificate.[189] A party may apply to the Federal Court of Appeal for an order varying or cancelling the certificate.[190] In considering the application, the judge may receive into evidence anything that, in the opinion of the judge, is reliable and appropriate, even if it would not otherwise be admissible under Canadian law,[191] and may make orders varying, cancelling or confirming the certificate.[192] A determination made by a judge in relation to the Attorney General's certificate is final and is not subject to review or appeal by any court.[193] Presumably, if the Attorney General's certificate is cancelled or varied in a way that would result in the disclosure of information which the Attorney General believes threatens national defence or national security, the option to discontinue those proceedings remains available to the Attorney General.[194]

8.92 As discussed in Chapter 7, a judge presiding at a criminal trial has general authority to make orders to ensure the right of an accused to a fair trial.[195] Such orders include:

> (a) an order dismissing specified counts of the indictment or information, or permitting the indictment or information to proceed only in respect of a lesser or included offence;
>
> (b) an order effecting a stay of the proceedings; and
>
> (c) an order finding against any party on any issue relating to information the disclosure of which is prohibited.

8.93 In *The Attorney General of Canada and Nicholas Ribic and The Attorney General of Ontario*,[196] Lutfy ACJ of the Federal Court of Canada heard the first application under s 38 of the *Canada Evidence Act* commenced since the recent amendments to the Act. The Attorney General of Canada sought an order under the Act confirming the

---

188 Ibid, s 38.13(1). The Act sets out the persons on whom the Attorney General must serve the certificate, which include, among others, the person presiding at the proceedings to which the information relates, every party to the proceedings, and the court who hears an appeal in relation to an order made under s 38.06(1)–(3) in relation to the information: see *Canada Evidence Act* [RS 1985, c C–5], s 38.13(3).

189 *Canada Evidence Act* [RS 1985, c C–5], s 38.13(5).

190 Ibid, s 38.131(1).

191 Ibid, s 131(5).

192 See Ibid, s 131(8)–(10).

193 Ibid, s 131(11).

194 The Australian Government Attorney-General's Department has noted that, in this way, the Canadian Act affords the Government absolute control over whether the information is disclosed in the course of a criminal proceeding: Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

195 These orders are to comply with the terms of any order made under *Canada Evidence Act* [RS 1985, c C–5], s 37(4.1), (5) and (6) which are discussed at [8.87] above.

196 *The Attorney General of Canada and Nicholas Ribic and The Attorney General of Ontario* (2002) FCT 839. Ribic was accused of hostage taking and, if convicted, was liable to life imprisonment. This case is also discussed in Ch 7 at [7.100] above.

prohibition of disclosure of five documents in the possession of the Department of Defence alleged to contain 'potentially injurious information' or 'sensitive information' as defined in s 38 of the Act. The presiding judge in the criminal proceedings had ordered that the five documents be fully disclosed to the defence, triggering notification to the Attorney General under the Act. Lufty ACJ stated that he was satisfied that each of the documents contained information which, if disclosed, would injure international relations, national defence or national security. He was also satisfied that four of the five documents contained information received by the Department of Defence on the basis that it would not be publicly disclosed. However, he emphasised that the Act required him to consider whether the public interest in disclosure outweighed the public interest in non-disclosure. He said:

> The new statutory language makes clear that the designated judge may authorize the disclosure of all or part of the information in severed or summary form where, after an assessment of the competing interests, the public interest in disclosure so warrants.
>
> In this case, the public interest in disclosure is to assure a fair trial where the accused faces serious charges and, if convicted, the possibility of a substantial penitentiary sentence. …
>
> The applicant's affidavit evidence asserts in strong and general terms the injury caused by making public the information in the five secret documents, even when sources are not identified. However, those assertions are not cast in the context of the disclosure of partial information for a fair trial in a serious criminal matter. Parliament has required the designated judge to balance competing interests, not simply to protect the important and legitimate interests of the state.[197]

8.94 After inspecting the documents, Lutfy ACJ concluded that four of the documents did not warrant disclosure.[198] In respect of the other, however, he concluded that portions of the document should be disclosed with the substitution of two words and that that information should be made public in a new expurgated document rather than by way of summary.[199]

8.95 By contrast, in *Her Majesty The Queen and the Attorney General of Quebec and Jaggi Singh and Jonathan Aspireault-Masse*, Hugessen J, in an application pursuant to s 38 of the *Canada Evidence Act*, ordered that part of the information that the Attorney General had objected to being disclosed on the ground of national security be released in the form of a summary.[200] The actual text of the summary to be disclosed was set out

---

197 Ibid.

198 This was on the basis that they were either of such little relevance to the criminal proceedings that the public interest in disclosure could not prevail or of no relevance to the criminal proceedings or that the information contained within them could be of no assistance to either party.

199 *Canada Evidence Act* [RS 1985, c C–5], s 38.06(2) envisages the disclosure of part of the information in expurgated or summary form.

200 The respondents were charged with taking part in a riot at the meeting of the G20 in Montreal. Following a disclosure session, the Attorney General objected to an order made by a judge that the prosecution disclose the names, registrations and written proofs of evidence of all Sûreté du Québec (SQ) officers who were present at the riot in plain clothes and anonymous: *Her Majesty The Queen and The Attorney General of Quebec and Jaggi Singh and Jonathan Aspireault-Masse* (2002) FCT 460, [1], [2].

in the judgment.[201] *Ribic* and *Singh* demonstrate the role of the court in approving the use of alternatives to full disclosure.

8.96 The *Canada Evidence Act* also provides for prosecutions not instituted by or on behalf of the Attorney General of Canada (for example, by provincial authorities) where sensitive information or potentially injurious information may be disclosed. In such cases, the Attorney General may issue and serve a fiat on the prosecutor which establishes the authority of the Attorney General with respect to the conduct of the prosecution.[202] Under these provisions, it appears that the Attorney General could opt to discontinue any proceedings where the court has ordered the disclosure of sensitive or potentially injurious information.

8.97 The ALRC's view at this stage is that, in matters involving classified or security sensitive information where the Government is not a party to the proceedings or is not the informant in the proceedings, there is merit in adapting that part of the Canadian model which requires the parties to notify the Attorney-General when they are required to disclose, or expect to disclose or cause the disclosure of classified or security sensitive information in court or tribunal proceedings. The Attorney-General would then have an opportunity to make representations and submissions to the court, ex parte if necessary, in relation to the disclosure of the information or the form, if any, that disclosure should take, or the conditions which should be imposed on any court-ordered disclosure. See Proposal 10–7.

Confidentiality undertakings and orders

8.98 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. Confidentiality undertakings are used routinely in litigation to protect commercially sensitive information. The following mechanisms, either alone or in combination, are some 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 …

---

201 See Ibid, [5], which sets out the summary of information to be disclosed as ordered on 22 March 2002, and [11], which sets out a further paragraph to the summary ordered to be disclosed by Hugessen J on 24 April 2002. Hugessen J also ordered disclosure of the number of plain clothes SQ officers present at the riot, stating that '[a]lthough there is slight risk that disclosure of this information will reveal the scope of the operation, I consider that the risk is minimal compared to the importance the information might have for the defence at the trial of the respondents.'

202 *Canada Evidence Act* [RS 1985, c C–5], s 38.15(1) and (2).

- The documents may be edited or 'blacked out' in order to delete highly confidential information such as company's financial data.[203]

8.99 The use of undertakings as a method of protecting classified and security sensitive information has received support from legal circles. In response to the Australian Government's proposal to introduce security clearances for legal aid lawyers representing defendants in national security cases (see Chapter 6), lawyers have asserted that they are often called upon to keep court matters confidential and can be bound by undertakings to the court.[204]

8.100 The Victorian Bar 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.[205]

8.101 The New South Wales Bar Association 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]'.[206]

8.102 The NSW Law Society submitted that:

> As the Victorian Bar and the NSW Bar Association have noted, it is commonplace for undertakings to be given in situations where sensitive material is before a court or tribunal. There is no evidence to suggest that this has been abused or that prosecution for contempt or professional misconduct are not adequate remedies in the event of any breach.[207]

8.103 The Law Council of Australia submitted that it:

> considers that the supervisory role of the court is generally adequate to deal with breaches of undertakings involving the protection of security information. Where a

---

203 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> at 7 March 2003.

204 I Munro, 'Fight Looms on Security Checks', *The Age* (Melbourne), 5.

205 The Victorian Bar, *Submission CSSI 1*, 8 April 2002. Victoria Legal Aid agreed with the submission of the Victorian Bar and submitted that '[u]ndertakings are an efficient, effective and proven way to ensure that information that arises in court remains confidential': Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003. 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.

206 New South Wales Bar Association, *Submission CSSI 2*, 11 April 2003.

207 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

> court imposed secrecy order is made the sanctions for contempt of court should be sufficient.[208]

8.104 However, the Attorney-General's Department argued that relying solely on confidentiality undertakings gives insufficient regard to the Commonwealth protective security policy. It submitted that:

> The effectiveness of confidentiality undertakings that are given to protect security classified information is questionable. Confidentiality undertakings are more punitive than preventative in nature. The resulting damage from a breach of confidentiality, particularly if it relates to unauthorised disclosure of evidence with top-secret classification, can be severe. In addition, undertakings do not give sufficient regard to the possibility that information may have been received from overseas on the condition that the person accessing the information has an appropriate security clearance. Undertakings are unlikely to be accepted as an effective means of protecting security classified information by foreign agencies who will then refuse to allow the Commonwealth to rely on their information in court. There is also a serious risk that countries who have concerns about Australia's capacity to adequately protect foreign sourced classified information will not be prepared to share intelligence material with Australia.[209]

8.105 Mr Lex Lasry QC, who represented Simon Lappas at his eventual trial, declined to seek a security clearance and the trial went ahead on the basis of undertakings.[210] Lasry was authorised by the Commonwealth to have access to a number of documents including the brief of evidence and the documents which were the subject of the various indictments. The terms of that undertaking are set out in full in Appendix 4.

8.106 The Victorian Bar noted that, simply because a person is charged with an offence related to national security does not mean that the entire prosecution brief is classified. The Victorian Bar expressed the view that undertakings are the best mechanism to protect documents as they are specific to the case and the parties in question, and are entered into by legal practitioners mindful of what should be protected in the particular circumstances.[211]

8.107 In the ALRC's view, confidentiality undertakings and security clearances should not necessarily be regarded as clear alternatives, and serve somewhat different purposes. Irrespective of whether a person already has, or is required to obtain, a security clearance in order to access classified and security sensitive information in court proceedings,[212] the ALRC is attracted to the idea that confidentiality undertakings can be tailored to the specific information in need of protection, thereby directing the attention of those giving the undertaking to their specific obligations.[213] A security clearance of itself does not meet this need. The undertaking in *Lappas* set out in Appendix 4 illu-

---

208 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.
209 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
210 The Victorian Bar, *Consultation*, Melbourne, 26 May 2003.
211 Ibid.
212 See the discussion on security clearances in Ch 6.
213 See Proposal 10–23 in Ch 10.

strates a number of preventative aspects of the undertaking including focus on the proper handling of the classified material. This focus would help militate against inadvertent lapses in the secure handling of this material that anyone with or without a security clearance may commit.

8.108 The court could require a confidentiality undertaking from, or make a confidentiality order binding on, not only lawyers instructed in proceedings involving classified or security sensitive information but the parties to the case, including an accused in criminal proceedings,[214] as well as witnesses and other participants in the proceedings. For example, 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.[215]

8.109 The Rules of the Federal Court of Australia, O 35, r 11, provide that, where a person (whether a party or not) fails to fulfil a binding undertaking to the Court to do or refrain from doing any act, following a motion by any party to enforce the undertaking, the Court is to make the order that the person do or refrain from doing the undertaken act. The rule does not affect the powers of the Court to punish a person for contempt. In the context of confidentiality undertakings to protect classified and security sensitive information, it would appear that the efficacy of O 35, r 11 is somewhat limited. Where a person divulges or publishes sensitive information that they have undertaken not to divulge or publish, the damage is done, and any enforcement of the undertaking would be restricted to restraining further breaches. Such circumstances would warrant the court exercising its powers to punish for contempt.

8.110 Breach of an undertaking to protect commercially sensitive information, where that breach amounts to a contempt of court, could found an action for damages by a third party against the party who breached the undertaking. For example, if the disclosure of the information caused a commercial transaction to collapse, the damages could be substantial. By contrast, any breach of an undertaking to protect classified or secu-

---

214 As noted in [8.57] in the US, the *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 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'. In the trial of Brian Regan in the USA, individuals to whom classified information was disclosed entered into a memorandum of understanding which read in part: '1. I agree that I shall never divulge, publish or reveal, either by word or conduct, or by any other means, such classified information and documents unless specifically authorized in writing to do so by an authorized representative of the United States Government, or as required by the Classified Information Procedures Act, or as provided for in the Protective Order entered in this case. 2. I understand that this agreement and any other nondisclosure agreement will remain binding upon me after the conclusion of the proceedings in this case.' See Memorandum of Understanding in *United States of America v Brian Patrick Regan* (USDC for the Eastern District of Virginia, case no 01–944–M).

215 For example, in the 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> at 7 February 2003.

rity sensitive information is likely to be irreparable and not properly compensated by any amount of damages.

8.111 Apart from express undertakings, parties to litigation are subject to an implied undertaking to the court not to use or disclose information received 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.[216] The primary purpose of implying such an undertaking is to protect the privacy of a party subject to the processes of the court and to encourage full and frank disclosure in litigation.[217] A breach of this undertaking (for example, by disclosing the information to the media or for the purpose of another court case) amounts to a contempt of court.[218] The Supreme Court of Victoria recently held that an implied undertaking does not necessarily cease upon the information being admitted into evidence in open court,[219] contrary to earlier authority for that proposition.[220] The Court stated:

> Where documents are provided to a party to litigation under some coercive process of the court with the result that the implied undertaking attaches to the effect that, without the leave of the court, they not be used otherwise than for the purposes of the litigation, the party bound by that undertaking is not freed of it simply because the document in question is marked as an exhibit in the proceeding in the course of which it was provided. To the extent that knowledge of the document has become public by dint of its tender in open court, members of the public will be free to make use of that knowledge as they will (subject always of course to any order specially made protecting confidentiality and the like), but the party affected by the undertaking remains bound as to use of the document itself. The distinction seems to us a valid one between, on the one hand, use of the documents the contents and the provenance of which are known in detail to the party by virtue of a privilege extended to it by the processes of the court and, on the other hand, use of the information about it which comes to the knowledge of the public by reason of the proceedings in open court (and during which, it may be supposed, the document is marked as an exhibit). The knowledge of the one cannot be equated with the knowledge of the other.[221]

---

216 Australian Government Solicitor, *Legal Briefing Number 56: Contempt of Court—How it Can Affect You*, <www.ags.gov.au/publications/briefings/br56.html> at 25 June 2000.

217 *British American Tobacco Australia Services Ltd v Cowell (as representing the estate of Rolah Ann McCabe, deceased)* [2003] VSCA 43, [20].

218 Australian Government Solicitor, *Legal Briefing Number 56: Contempt of Court—How it Can Affect You*, <www.ags.gov.au/publications/briefings/br56.html> at 25 June 2000.

219 *British American Tobacco Australia Services Ltd v Cowell (as representing the estate of Rolah Ann McCabe, deceased)* [2003] VSCA 43.

220 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.

221 *British American Tobacco Australia Services Ltd v Cowell (as representing the estate of Rolah Ann McCabe, deceased)* [2003] VSCA 43, [48]. The Court continued: 'The contrast is only the greater if the documents have been put before the court by means of an affidavit to which they are exhibited; the affidavit becomes evidence, together with its attendant exhibits, once it is relied upon in open court but not uncommonly that does little or nothing to publicise the contents of the documents exhibited, to which only passing reference may happen to be made in the affidavit. Moreover, exhibits are not normally avail-

8.112 The Supreme Court noted that the use of discovered documents in an interlocutory proceeding may not always be as significant as their use at trial.[222] It stated that it would be absurd if the use of a discovered document as an exhibit to an affidavit and relied upon by an opponent in the course of an interlocutory application to have the document ruled admissible at trial operated to bring the implied undertaking to an end.[223]

8.113 The Rules of the Federal Court 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.[224] [emphasis added]

8.114 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.

8.115 Courts and tribunals can also make orders to protect the confidentiality of classified and security sensitive information by restricting access to the documents containing it.[225] 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.[226] 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.'[227] 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:

---

able for inspection': *British American Tobacco Australia Services Ltd v Cowell (as representing the estate of Rolah Ann McCabe, deceased)* [2003] VSCA 43, [36]. [citations omitted]

222 *British American Tobacco Australia Services Ltd v Cowell (as representing the estate of Rolah Ann McCabe, deceased)* [2003] VSCA 43, [47].

223 See Ibid, [46].

224 *Federal Court Rules*, O 15 r 18.

225 For example, the court can restrict access to information and make suppression orders under the *Crimes Act 1914* (Cth), s 85B(1)(b) and (c) and the *Criminal Code Act 1995* (Cth), s 93.2(b) and (c). See discussion at [8.212]–[8.213].

226 Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), 27.

227 Ibid, 27.

> 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.[228]

8.116 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.[229]

8.117 Presumably, any disclosure of classified and security sensitive information in breach of an undertaking or order could also constitute a criminal offence under one or more of the relevant provisions in the *Crimes Act 1914* (Cth), *Criminal Code Act 1995* (Cth) or other federal legislation: see Chapter 5.

Blocking disclosure or admission of evidence

Public interest immunity

8.118 A claim of public interest immunity (also called state interest immunity) is one of the most common ways in which classified and security sensitive information can be protected in court proceedings.

8.119 Public interest immunity differs from other mechanisms to protect sensitive evidence in that it generally operates to exclude the information completely, rather than limiting or protecting its disclosure to the public or parties to the proceedings while it is being used in court. A claim for public interest immunity can, therefore, go to the very heart of the case, as in the *Lappas* prosecution.[230]

8.120 The Terms of Reference ask the ALRC to consider the operation of 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.[231]

8.121 There is no real dispute that some information, the disclosure of which would affect national security or other critical state interests, should be protected from release. This section looks at 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.

---

228 Ibid, 28.

229 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.

230 This case is also summarised in Appendix 4.

231 Section 130 is set out in full in Appendix 3.

Common law public interest immunity

8.122 The common law formulation of public interest immunity is stated 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.[232]

8.123 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.[233]

8.124 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, whereas a claim of public interest immunity can be made by the state, a non-governmental party to the proceedings 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.[234] 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.[235]

8.125 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 or covert operatives.[236]

8.126 There is a general presumption under the common law that disclosure of classified and security sensitive information would be prejudicial to the public interest.[237] Mason J stated in *Church of Scientology v Woodward* that:

> [N]o one could doubt that the revelation of security intelligence in legal proceedings would be detrimental to national security.[238]

8.127 However, this privilege is not unqualified—in particular, in cases where the information concerned may be of direct use to the defendant. In *Alister v R*, the High

---

232 *Sankey v Whitlam* (1978) 142 CLR 1, 38 (Gibbs ACJ).
233 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 350.
234 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 597.
235 *Cooke v Maxwell* (1817) 171 ER 614, 615.
236 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 597.
237 B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 14.
238 *Church of Scientology v Woodward* (1982) 154 CLR 25, 59 cited in B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 15.

Court considered it important that the documents sought from ASIO (should they exist) would support the defence of an accused in criminal proceedings.[239] In that case ASIO eventually disclosed the documents in question to the Justices of the High Court and a public interest immunity claim was upheld to prevent disclosure to the defendant.

8.128 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.[240] This may be one way to meet the risk of greymail as a party's threat to disclose, or wish to gain access to, classified or security sensitive information will be defeated unless the court is satisfied that that party has a legitimate purpose or need to do so.

Evidence Act 1995 (Cth)

8.129 In the commentary on the common law doctrine of public interest immunity in its interim report *Evidence*,[241] 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.[242] However, the ALRC did recommend a change from the (then) accepted common law formula which required the judge, when 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'.[243]

8.130 The *Evidence Act 1995* (Cth) substantially reflects the ALRC's recommendations. Section 130(1) provides:

> 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.[244]

8.131 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; s 130(4) provides that:

---

239 *Alister v R* (1983) 50 ALR 41, 46 cited in B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 15.

240 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 474.

241 Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985).

242 Ibid, 490.

243 Ibid, 491, citing *Alister v R* (1983) 50 ALR 41, 44–45 (Gibbs CJ).

244 The *Evidence Act 1995* (Cth) applies in all federal courts and in the courts of the ACT. The *Evidence Act 1995* (NSW) mirrors the Commonwealth Act, and contains a provision identical to s 130.

> Without limiting the circumstances in which information or a document may be taken for the purposes of subsection (1) to relate to matters of state, the information or document is taken for the purposes of that subsection to relate to matters of state if adducing it as evidence would:
>
> (a) prejudice the security, defence or international relations of Australia;
>
> (b) damage relations between the Commonwealth and a State or between 2 or more States; or
>
> (c) prejudice the prevention, investigation or prosecution of an offence; or
>
> (d) prejudice the prevention or investigation of, or the conduct of proceedings for the recovery of civil penalties brought with respect to other contraventions of the law; or
>
> (e) disclose, or enable a person to ascertain, the existence or identity of a confidential source of information relating to the enforcement or administration of a law of the Commonwealth or a State; or
>
> (f) prejudice the proper functioning of the government of the Commonwealth or a State.

8.132 These factors are consistent with those developed by the prior common law.[245] In *State of NSW v Ryan*,[246] 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*[247] and the provisions of s 130.[248] Similarly, von Doussa J held in *Chapman v Luminis Pty Ltd (No 2)*[249] that the common law principles considered in *Aboriginal Sacred Sites Protection Authority v Maurice*[250] continue to apply under s 130.[251]

8.133 Section 130(1) indicates that the onus is on the party seeking to preserve the secrecy of matters of state to show that this factor outweighs the public interest in admitting the information or document into evidence.[252] This reflects the common law in that it does not confer absolute immunity on information relating to matters of state

---

245 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 470.

246 *State of NSW v Ryan* (1998) 101 LGERA 246.

247 *Sankey v Whitlam* (1978) 142 CLR 1.

248 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 472.

249 *Chapman v Luminis Pty Ltd (No 2)* (2000) 100 FCR 229.

250 *Aboriginal Sacred Sites Protection Authority v Maurice* (1986) 10 FCR 104.

251 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 475.

252 S Odgers, *Uniform Evidence Law* (4th ed, 2000), 343.

or an absolute right to protect the information,[253] and appears to apply to both oral and documentary evidence.[254]

8.134 The ALRC also listed the considerations which should guide the courts in balancing the public interests 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.[255]

8.135 These considerations were implemented in s 130(5), which, without being exhaustive, lists the matters the court is to take into account for the purpose of determining the balance on the public interest:

> (a) the importance of the information or document in the proceeding;
>
> (b) if the proceeding is a criminal proceeding—whether the party seeking to adduce evidence of the information or document is a defendant or a prosecutor;
>
> (c) the nature of the offence, cause of action or defence to which the information or document relates, and the nature of the subject matter of the proceeding;
>
> (d) the likely effect of adducing evidence of the information or document, and the means available to limit its publication;
>
> (e) whether the substance of the information or document has already been published;
>
> (f) if the proceeding is a criminal proceeding and the party seeking to adduce evidence of the information or document is a defendant—whether the direction is to be made subject to the condition that the prosecution be stayed.

8.136 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 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;[256] whether a representative of government has supported the non-disclosure of the information or document; the subject matter of the information or document; whether the information or document has con-

253 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 469.
254 Ibid, 471.
255 Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985), 491.
256 See [8.160].

temporary importance or is only of historical interest; and whether the information or document was acquired on the basis that it would be kept confidential.[257]

8.137 While the Act is in most respects a restatement of the common law, it only applies to the admission of evidence at a trial or a hearing.[258] Therefore, the common law would still apply 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 position is different in New South Wales courts, where rules of court extend the operation of s 130 to ancillary processes.[259]

8.138 As noted at [8.118], public interest immunity under the *Evidence Act* operates as a device to exclude evidence completely—by virtue of s 134, evidence that must not be adduced or given in a proceeding because of public interest immunity is not admissible in that proceeding.

8.139 A number of matters required clarification following the enactment of s 130. For example, 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 about whether public interest immunity would be limited strictly to categories of governmental matters.[260] In *R v Young*, Spigelman CJ 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'.[261]

8.140 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;[262] and whether and how courts should distinguish between the public and private activities of the state.[263]

State and territory legislation

8.141 The *Evidence Act 1995* (Cth) applies in all federal courts and, with the agreement of the Australian Capital Territory, the courts of the ACT. In June 1995, New South Wales enacted similar legislation in the *Evidence Act 1995* (NSW).

---

257 S Odgers, *Uniform Evidence Law* (4th ed, 2000), 342.

258 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 599.

259 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 468. For example, in relation to civil proceedings, see *Supreme Court Rules* (NSW), Pt 23 (Discovery and Inspection of Documents).

260 S Odgers, *Uniform Evidence Law* (4th ed, 2000), 341.

261 *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), 471.

262 S Odgers, *Uniform Evidence Law* (4th ed, 2000), 342.

263 J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002), 471.

8.142 The general law of evidence in the other States and Territory is a mixture of some implementation of the Commonwealth provisions, common law and some codified provisions. In relation to public interest immunity, essentially the common law principles are retained in all jurisdictions either through codification (in the case of New South Wales and the ACT) or direct operation. There are a few procedural differences operating in some jurisdictions.

8.143 In the Northern Territory, the issuing of ministerial certificates (also discussed at [8.183]) is allowed in certain circumstances. Section 42D of the *Evidence Act 1939* (NT) allows the Attorney-General to certify that, in his or her opinion, the disclosure of the contents of a document or record in legal proceedings described in the certificate is not in the public interest because it would disclose communication between members of the Executive Council and/or Ministers.[264]

8.144 In Queensland, under the *Evidence Act 1977*, witness anonymity certificates may be issued to protect persons who are covert law enforcement operatives.[265] Section 192 of the *Crime and Misconduct Act 2001* (Qld) allows a witness to make a claim for public interest immunity in refusing to answer a question in a hearing of the Crime and Misconduct Commission.

8.145 In Victoria, s 391A of the *Crimes Act 1958* (Vic) expressly sets up a pre-hearing procedure that may settle evidentiary matters such as public interest immunity claims (discussed at [8.118]).

> Where an accused person is arraigned on indictment or presentment before the Supreme Court or the County Court the Court before which the arraignment takes place, if the Court thinks fit, may before the impanelling of a jury for the trial hear and determine any question with respect to the trial of the accused person which the Court considers necessary to ensure that the trial will be conducted fairly and expeditiously and the hearing and determination of any such question shall be conducted and have the same effect and consequences in all respects as such a hearing and determination would have had before the enactment of this section if the hearing and determination had occurred after the jury had been impanelled.

Making a claim for public interest immunity

8.146 A claim for public interest immunity at common law can be made at any stage of proceedings, including issuing and answering subpoenas, ordering inspection following discovery, or in examining witnesses.[266] As noted above, s 130 of the *Evidence*

---

264 Section 42G notes that s 42D does not limit the prerogatives of the Crown or the operation of any law requiring a court to prohibit the disclosure of a written or oral communication on the grounds that it is in the public interest to do so.

265 *Evidence Act 1977* (Qld), s 21D. See also [8.43] above.

266 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 352.

Act applies only to the admission of evidence, not pre-trial procedures, except in New South Wales.[267]

8.147 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.[268] Subsequent development of the rule extended the right to claim beyond a strictly prerogative right of the Crown to other litigants and interested people.[269] Claims may now be made by a party to proceedings, a witness or the state.

8.148 Generally, a claim to public interest immunity is made before trial in response to a warrant or subpoena, or in anticipation of a general right to inspect documents.[270] A claim can also be made in relation to a witness's testimony, either before or during trial.[271] One view is that a public interest immunity claim should be considered a separate action or *lis* between the parties, distinct from the main action.[272] If that is so, any appeal from a public interest immunity determination would have to be resolved before the trial could commence or continue.

8.149 The claim for immunity is usually supported by one or more affidavits, generally sworn by the responsible Minister or a senior public servant.[273] Cross-examination of the deponent and presentation of counter-evidence is generally not allowed as this would, in effect, defeat the purpose of keeping the information in question out of the proceedings.[274]

8.150 If the court is not satisfied of the claim from the affidavit evidence, it may seek further information, or in rare cases may examine the documents in private. Courts have indicated that this power should be used rarely, and only exercised where it appears to the court, on balance, that the documents should be produced.[275]

8.151 The Attorney-General's Department Legal Services Directions deal briefly with public interest immunity issues. The Directions state that, regardless of which agency is involved in the litigation, where a public interest immunity claim could be made about information for which another agency has administrative responsibility, the agency conducting the litigation must refer the question of whether to make a claim to the public interest immunity agency[276] or that agency's Minister. If the claim is resisted

---

267 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 599. See *Supreme Court Rules* (NSW), Pt 23 (Discovery and Inspection of Documents).

268 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 353.

269 *Sankey v Whitlam* (1978) 142 CLR 1, 44 (Gibbs ACJ).

270 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 362.

271 Ibid, 362.

272 B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 5.

273 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 363.

274 B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 8.

275 Ibid, 9 citing *Sankey v Whitlam* (1978) 142 CLR 1, 46.

276 That is, the agency with ownership of the information for which public interest immunity is sought.

by another party in the litigation, the public interest immunity agency is responsible for handling the claim, in consultation with the agency handling the litigation (such as the DPP).

Differences between criminal and civil matters

8.152 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.[277] In criminal cases, courts are more readily prepared to inspect documents to determine if public interest immunity applies.[278] In *Alister v The Queen*, Brennan J 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.[279]

8.153 In criminal proceedings, an accused's interest in obtaining exculpatory material 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.[280] This interest can outweigh a general public interest against disclosure of police information[281] and state papers where a person's liberty is at stake.[282] This principle also applies in regard to sources of police information, except documents and other evidence involving vital state interests.[283]

8.154 Similarly, the informer rule is treated differently in criminal trials if the accused demonstrates that disclosure of the identity of the informer could materially assist the defence, whether by establishing innocence or by raising a reasonable doubt.[284] This requirement to show relevance of the information to the defence is crucial. In *Alister*, the documents in question were inspected by the court, but then ultimately not disclosed to the defence on the grounds that they would be irrelevant.[285]

8.155 This illustrates a real difference between criminal and civil procedures. In committal proceedings in a criminal case, the prosecution must establish the elements of the offence, and the defence has the right to reserve elements of their defence for the trial itself. Where public interest immunity is an issue, the defence may be required to reveal its defence early in the proceedings in order to show relevance. One way to

---

277 *Alister v R* (1983) 50 ALR 41, 81 (Brennan J).
278 S McNicol, *Law of Privilege* (1992), 394–5.
279 *Alister v R* (1983) 50 ALR 41, 81 (Brennan J).
280 *Marks v Beyfus* (1890) 25 QBD 494, 498 (Lord Esher MR), cited in *Sankey v Whitlam* (1978) 142 CLR 1.
281 *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.
282 *Sankey v Whitlam* (1978) 142 CLR 1.
283 *Rogers v Home Secretary* [1973] AC 388, 407, cited in D Byrne and J Heydon, *Cross on Evidence: Australian Edition* (1996), [27043].
284 *R v Keane* [1994] 2 All ER 478, cited in D Byrne and J Heydon, *Cross on Evidence: Australian Edition* (1996), [27043].
285 *Alister v R* (1983) 50 ALR 41.

overcome this unfairness might be to allow the defence to present its defence ex parte to the court. Alternatively, an independent counsel or amicus curiae might be used to examine the documents and argue before the court the reasons favouring disclosure.[286]

8.156 In civil proceedings, the test of relevance remains but the discovery procedures are markedly different. Where the Government 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.[287] The party seeking to satisfy that onus must do so without access to the documents in question.[288]

8.157 Public interest immunity is a crucial aspect of civil proceedings involving national security. However, a successful Government 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.[289] 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.[290]

> 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.[291]

8.158 A heavy burden may be placed on the non-government party 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.[292]

---

286 I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html> at 12 June 2003, 12.

287 *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.

288 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 366.

289 Ibid, 337.

290 L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), 337.

291 Ibid, 331.

292 Ibid, 332.

8.159 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. However:

> 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.[293]

Class claims and contents claims

8.160 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 papers.

8.161 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.[294] The argument advanced was that public servants must be allowed to give candid advice without fear, in the interests of good government. 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 adopted.[295]

8.162 Can (or should) 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.[296] 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.[297]

---

293 *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.

294 I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html> at 12 June 2003, 4.

295 Ibid, 4.

296 *Sankey v Whitlam* (1978) 142 CLR 1, 57 (Stephen J).

297 *Alister v R* (1983) 50 ALR 41, 64 (Wilson and Dawson JJ).

8.163 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.[298] 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's claims.[299]

Submissions and consultations

8.164 As noted above, public interest immunity may be claimed in order to protect various types of government information. The ALRC has been told that it is estimated that public interest immunity arises as an issue in less than one per cent of cases across all courts.[300] In these cases, it is commonly used to protect the identity of police informers. It is common ground among the experts consulted by the ALRC that the seeking of public interest immunity on the basis of national security was rare.[301]

8.165 There is no question that classified and security sensitive information falls squarely within the ambit of public interest immunity, as the public interest in protecting genuine matters of national security is clear. Further, following the release of BP 8,[302] no consultation or submission has suggested that courts have been unduly reluctant to uphold public interest immunity claims.

8.166 However, the *Lappas* case has highlighted the deficiencies with public interest immunity as a method of protecting classified and security sensitive information. In that case, the Crown sought to rely on public interest immunity to allow it to use 'empty shells' of two of the central documents in the proceedings and to provide only very general oral summaries of their contents. The trial judge upheld the claim for public interest immunity. However, because the defence could not then properly give evidence related to the contents of those documents and because s 134 of the *Evidence Act 1995* (Cth) prevented any secondary evidence of the documents' contents being admitted into evidence, the prosecution on one of the charges against Lappas was stayed.[303]

8.167 The Attorney-General's Department has submitted that public interest immunity is a recognised means of protecting security classified information and should remain an element of any regime which seeks to protect such information. However, the Department identified a number of limitations in the protection offered by public interest immunity:

- Public interest immunity does not overcome procedural gaps in the protection of security classified information. For example, public interest immu-

298 Ibid, 64 (Wilson and Dawson JJ).
299 S McNicol, *Law of Privilege* (1992), 406.
300 B Leader, *Consultation*, By telephone, 26 August 2003.
301 Ibid; J Renwick, *Consultation*, Sydney, 9 September 2003.
302 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003).
303 *R v Lappas and Dowling* [2001] ACTSC 115. A summary of the case can be found in Appendix 4.

nity does not impose a notification requirement on the defence or mandate closed hearings.

- Public interest immunity does not provide the courts with clear authority to permit summaries or stipulations to be adduced in place of a document or information in question.

- Public interest immunity as provided for in s 130 of the *Evidence Act 1995* (Cth) only applies during trial and not during pre-trial hearings (for example, committals). Claims made during pre-trial hearings must rely on the common law principles governing public interest immunity claims. This can result in greater uncertainty, the application of the common law often being less clear than the application of a legislative provision.[304]

8.168 The Law Council of Australia submitted that existing rules relating to public interest immunity, whether at common law or under s 130 of the *Evidence Act 1995* (Cth), could be improved. The Law Council considers that the practical application of public interest immunity law is difficult and complex, and that some further work on the systematisation of the various circumstances involving public interest immunity would be valuable.[305]

8.169 Commentators have also highlighted difficulties with establishing clear procedures for the determination of a public interest immunity claim when the issues of a case have not yet emerged at the beginning of the proceedings. Once a case for the maintenance of secrecy in the public interest is made out, the court must weigh this against the interest in disclosure in the case at hand. Where the information forms a significant part of the case, its disclosure or otherwise could have profound impact. If the issues of the case are not clear from the beginning, the court may provisionally deny access until the trial is underway or pleadings finalised.[306] This could lead to some uncertainty regarding the level of protection that the information will ultimately receive, although presumably the court would not alter the degree of protection granted without an opportunity for all parties and the Government to be heard on the question first.

8.170 In the *Evidence* report, the ALRC found that it was important to maintain the supervisory role of the courts.

> It cannot be assumed that all claims are justified. To abandon the supervisory role of the courts would 'come close to conferring immunity from conviction upon those who may occupy or may have occupied high offices of state if proceeded against in relation to their conduct in those offices'.[307]

304 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003, 25–26.
305 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.
306 A Ligertwood, *Australian Evidence* (3rd ed, 1998), 364.
307 Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985), 491 citing *Sankey v Whitlam* (1978) 142 CLR 1, 48 (Stephen J).

8.171 It has been suggested that the public interest immunity procedure has worked effectively to date.

> The balancing which is undertaken, between the public interests of (a) maintaining confidentiality for certain documents and (b) ensuring a fair and open trial with all relevant material placed before the tribunal, is, under the present law, undertaken case by case. The outcome depends upon the unique particular circumstances of the subject documents and of the issues in the relevant proceedings. It is difficult to see how the judgments which are necessary, from document to document and case to case, could be made any more satisfactorily under a different regime.[308]

8.172 Another consultation suggested that it would be unhelpful to make the categories of documents established in the Act more specific: 'if a judge uses them as a checklist, he or she will flush out the issues there'.[309]

8.173 In the *Evidence* report, it was noted that one issue in relation to public interest immunity was whether some procedural proposals should be included in the *Evidence Act* to enable a judge's ruling to be obtained in advance of the trial, and to allow time for an appeal from that ruling.[310] At the time of that report, the ALRC considered that the decision in *Sankey v Whitlam*[311]—where reference is made to the duty to defer inspection to enable the Attorney-General to appeal—provided a precedent for raising challenges in this area, and no specific proposal was made.[312] In the relevant passage in *Sankey*, Gibbs ACJ stated that, where a claim of public interest immunity is not upheld, given the potentially damaging nature of the material, the Government must be given the opportunity to appeal.

> If a strong case has been made out for the production of the documents, and the court concludes that their disclosure would not really be detrimental to the public interest, an order for production will be made. In view of the danger to which the indiscriminate disclosure of documents of this class might give rise, it is desirable that the government concerned, Commonwealth or State, should have an opportunity to intervene and be heard before any order for disclosure is made. Moreover, no such order should be enforced until the government concerned has had an opportunity to appeal against it, or to test its correctness by some other process, if it wishes to do so.[313]

8.174 One expert had called for more clearly defined appeal processes in relation to public interest immunity claims. Whilst noting the comments in *Sankey*, in practice the experience had been that the process for challenging such a decision is not always clear and, especially in criminal cases, can be quite difficult to establish.[314]

> Difficulties can arise in determining an available or appropriate method of appealing or otherwise testing a decision rejecting a privilege claim. Such a decision is usually

---

308 Advisory Committee member, *Correspondence*, 18 September 2003.
309 Justice T Smith, *Consultation*, Melbourne, 29 August 2003.
310 Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985), 492.
311 *Sankey v Whitlam* (1978) 142 CLR 1.
312 Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985), 492.
313 *Sankey v Whitlam* (1978) 142 CLR 1, 43.
314 B Leader, *Consultation*, By telephone, 26 August 2003.

> made in the course of hearing the proceedings in which the privilege claim is made and those proceedings often comprise a criminal trial. There are often statutory provisions precluding appeals from decisions made in the course of the proceedings (especially where the proceedings are in a lower court) or requiring leave to appeal.[315]

8.175 This was echoed in another consultation:

> [P]eople are looking for a procedure or guidelines so that the parties know in advance how the issues are to be dealt with, including any appeal process.[316]

8.176 A number of the cases have discussed a court's need to have sufficient knowledge of the information in issue to be able to determine its significance.[317] The ALRC agrees that judges would find it difficult to satisfy themselves otherwise unless they can cross-examine the deponent of an affidavit claiming public interest immunity or examine the documents themselves.

Commission's views

8.177 One way to deal with the difficulties raised in submissions and consultations would be to include classified and security sensitive information as a class of public interest immunity claim that must be upheld by the courts. Arguments in favour of class claims are essentially that they provide certainty and save judicial time by removing the need to perform the balancing exercise.[318] The basis for this class claim would be that any information which revealed the operations, practices, intelligence or communications of Australia's intelligence community or which prejudiced Australia's international relations must be granted automatic protection. Such protection could be achieved through either a statutory class protection (for example, in the *Evidence Act*) or by legislative provision for a ministerial certificate.[319] For example, the *Canada Evidence Act* contains a similar protection for Cabinet papers. Under s 39, a Minister or the Clerk of the Privy Council can object to the disclosure of information before a court (or other body able to compel evidence) by certifying in writing that the information constitutes a confidence of the Queen's Privy Council for Canada. Where such a certificate is issued, the protection of the information is automatic and not tested by the court.[320]

8.178 The ALRC has considered the desirability of according statutory protection to this class of documents. Although recognising the importance of protecting certain types of documents, Australian courts have been reluctant to say that an outright immu-

---

315 B Leader, 'Public Interest Privilege' (Paper presented at Australasian Government Solicitors' Conference, 19–20 November 2002 [Paper updated as at 20 March 1998]), 12.

316 Advisory Committee member, *Consultation*, Melbourne, 29 August 2003.

317 A Ligertwood, *Australian Evidence* (3rd ed, 1998).

318 I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html> at 12 June 2003, 4.

319 Leigh cites two examples of this: the *Interception of Communications Act 1985* (UK), s 9 and the *Canada Evidence Act* [RS 1985, c C–5]: I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html> at 12 June 2003, 5.

320 *Canada Evidence Act* [RS 1985, c C–5], s 39.

nity should apply. At this time, and without any submissions to the contrary,[321] the ALRC does not believe that creating a legislated class of public interest immunity for classified and security sensitive information is warranted.

8.179 At this stage of the Inquiry, it is the ALRC's view that any problems with public interest immunity lie not with the application of the legislation or a reluctance on the part of the judiciary to protect classified and security sensitive information. Rather, there are some procedural problems associated with the seeking of a public interest immunity claim, a restrictive lack of flexibility in procedural alternatives, and a lack of any clear appeal process. Much of the uncertainty may be attributed to the lack of guidance from the relatively sparse case law in this area.

8.180 The ALRC accepts the view that public interest immunity is a 'blunt instrument' insofar as it excludes evidence altogether. Regardless of how well it operates in some cases, it should be regarded as only one method of protecting classified and security sensitive information and cannot adequately serve all cases. Consequently, the ALRC proposes to list public interest immunity as one of a number of measures within the legislative regime for the protection of classified and security sensitive information proposed in Chapter 10. However, a conventional claim for public interest immunity under s 130 would remain.

8.181 As outlined in the Proposals in Chapter 10, a pre-trial procedure for a public interest immunity claim in the case of classified and security sensitive information would be established, including mechanisms for appeal. This, combined with the flexibility offered by the creation of other mechanisms to protect classified and security sensitive information, should substantially address the concerns raised in this Inquiry about public interest immunity.

8.182 Public interest immunity does not only operate in relation to classified and security sensitive information—indeed, it rarely does. As the ALRC has only looked at its operation in this context, it does not propose to amend s 130, but rather to leave the option open for the Government to seek protection under the s 130 regime or under the proposed new Act specifically dealing with classified and sensitive national security information. In this way, s 130 will continue to serve to exclude evidence of police informers, cabinet deliberations and similar sensitive (but not national security related) matters.

Ministerial certificates

8.183 The issuing of ministerial certificates in order to claim public interest immunity was common in the United Kingdom and Australia until the 1960s. In 1942, the House of Lords made a controversial decision—in the context of a world war—that courts

321 The Law Council of Australia submitted that 'a claim that a document belongs to a particular class by virtue of a security classification should not prevent judicial determination of the merits of a particular case': Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

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.[322] 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.[323]

8.184 In the UK, this doctrine was overturned in *Conway v Rimmer*.[324] This case established that a minister's certificate was no longer able to protect information in and of itself, and that a trial judge had to balance the state interest against the broader public interest. This approach has continued to be expanded in the UK cases. In *Air Canada v Secretary of State for Trade (No 2)*,[325] the House of Lords made it clear that even Cabinet papers regarding government policy would not be immune from disclosure where their contents went to the heart of the matter at issue.

8.185 In Australia, *Sankey v Whitlam* established that, as a matter of common law, ministerial certificate claims were not regarded as conclusive, with the court placed in the role of the ultimate guardian of public policy to ensure justice in each case.[326]

8.186 Following *Sankey v Whitlam*, in 1979 the NSW Parliament inserted Part VI into the *Evidence Act 1898* (NSW), which allowed a ministerial certificate claiming public interest immunity in relation to government communications to be conclusive in any legal proceeding. This move was widely criticised as an over-reaction to *Sankey* and the amendment was repealed in 1988,[327] with the NSW Attorney-General, John Dowd QC, commenting that: 'This legislation has been in effect for nine years; it should not remain one day longer than necessary'.[328] By removing Part VI, the NSW Government expressed a commitment to free and open government, and a desire to restore the independence of the courts.[329]

8.187 As noted above, s 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;[330] this is the only state or territory legislation to do so.

8.188 Ministerial certificates are a key part of the regime for protecting classified and security sensitive information in Canada. As discussed above, the *Canada Evidence*

---

322 See *Duncan v Cammell, Laird & Co* [1942] AC 264, discussed in M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 598.
323 M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998), 598.
324 *Conway v Rimmer* [1968] AC 910.
325 *Air Canada v Secretary of State for Trade* [1983] 2 WLR 529.
326 *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), 352.
327 *Evidence (Crown Privilege) Amendment Act 1988 (No 3)* (NSW). See S McNicol, *Law of Privilege* (1992), 396.
328 Ibid, 396 citing *Parliamentary Debates* (NSW), Legislative Assembly, 18 May 1988, 297 (Mr Dowd).
329 Ibid, 397 citing *Parliamentary Debates* (NSW), Legislative Assembly, 18 May 1988, 296 (Mr Dowd).
330 See [8.143] above.

Act provides that, if a court makes an order resulting in the disclosure of information that the Attorney General has sought to withhold on the grounds of public interest, the Attorney General may issue a certificate that prohibits such disclosure for the purpose of protecting, among other things, national defence or national security.[331] The effect of the certificate is that, notwithstanding any other provision in the Act, disclosure of the information is prohibited in accordance with the terms of the certificate.[332] A party may apply to the Federal Court of Appeal for an order varying or cancelling the certificate.[333] Where the Attorney General's certificate is cancelled or varied in a way that would result in the disclosure of information which the Attorney General believes threatens national defence or national security, the Attorney General may nonetheless discontinue those proceedings.

8.189 Conclusive certificates are part of the regime for exempting certain types of information from release under the *Freedom of Information Act 1982* (Cth) (FOI Act).[334] Under s 33(2) of that Act, a conclusive certificate may be issued by the relevant Minister which exempts a document from disclosure under the Act on the basis that it relates to national security, defence or international relations.[335]

8.190 Under s 55 of the Act, appeal may be made to the Administrative Appeals Tribunal (AAT) to review the issuing of a conclusive certificate. The role of the AAT in reviewing these certificates is not the same as the role of the courts in a public interest immunity case since the AAT does not consider whether the public interest in disclosure outweighs the public interest in non-disclosure. Rather, the AAT considers whether or not reasonable grounds exist (at the time of the hearing) for the claims made in the certificate.[336]

---

331 *Canada Evidence Act* [RS 1985, c C–5], s 38.13(1). The Act sets out the persons on whom the Attorney General must serve the certificate, which include, among others, the person presiding at the proceedings to which the information relates, every party to the proceedings, and the court who hears an appeal in relation to an order made under s 38.06(1)–(3) in relation to the information: see *Canada Evidence Act* [RS 1985, c C–5], s 38.13(3).

332 *Canada Evidence Act* [RS 1985, c C–5], s 38.13(5).

333 Ibid, s 38.131(1).

334 Freedom of information is discussed in more detail in Ch 3.

335 As outlined in s 33(1) of the FOI Act. Conclusive certificates may also be issued in relation to information about Commonwealth/State relations (s 33A), Cabinet documents (s 34), Executive council documents (s 35) and internal working documents which show government deliberations or processes (s 36).

336 Section 58(4) of the FOI Act states: 'Where application has been made to the Tribunal for the review of a decision to grant access to a document that is claimed to be an exempt document under section 33, 33A, 34 or 35 and in respect of which a certificate (other than a certificate of a kind referred to in subsection 5(A)) is in force under that section, the Tribunal shall, if the applicant so requests, determine the question whether there exists reasonable grounds for that claim'. See *Australian Doctors Fund Ltd v Department of Treasury and Commissioner of Taxation* (1993) 30 ALD 265; *Re Throssell and Department of Foreign Affairs* (1987) 14 ALD 296.

8.191 In BP 8, the ALRC sought views on the operation of ministerial certificates under the *Freedom of Information Act*.[337] No concerns regarding either their use or their ability to be challenged in the AAT were raised with the Commission.

8.192 The Law Society of NSW commented that any ministerial certificate to protect classified and security sensitive information should not be conclusive, but rather be subject to the scrutiny of the court or tribunal to which it is provided or by other review process, such as that provided for under the *Freedom of Information Act.*[338]

8.193 Conclusive ministerial certificates are also allowed in relation to the review of decisions by the Refugee Review Tribunal under s 411(3) of the *Migration Act 1958* (Cth). Under that section, the Minister may issue a conclusive certificate if he or she believes that it would be contrary to the national interest to change the decision or that it would be contrary to the national interest for the decision to be reviewed. The protection of sensitive information under the *Migration Act* is discussed in greater detail in Chapters 9 and 10.

Commission's views

8.194 Although ministerial certificates are not legislated for in Australia in relation to the disclosure of classified and security sensitive information in court proceedings, there is little substantive difference in practice between the regime under the *Canada Evidence Act* and the operation of public interest immunity in Australia—where a court decides not to accept the Government's argument for suppression, the option exists for the Government to withdraw the proceedings.

8.195 However, a clear statutory articulation of the options open to the Government in protecting national security information may be preferred. Legislating for the use of certificates is one way to ensure that the Government retains ultimate control over the disclosure of national security information, even if, ultimately, the only strategic choice that can be made is to discontinue proceedings.

8.196 However, at this stage the ALRC does not support the enactment of a provision for conclusive ministerial certificates. As a key part of the principle of executive accountability, the courts must be able to exercise an ultimate discretion to consider the material that should properly be brought into proceedings. The use of an unchallengeable certificate would reverse the considerable development of the law in this area. Importantly, no submission expressed support for the re-introduction of such certificates in court proceedings.

8.197 Ministerial certificates can create the perception that judges are merely 'rubber-stamping' the decision of the Attorney-General or Minister that certain evidence

337 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), 25 (Questions 7 and 8).

338 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

cannot be produced. The ALRC was told by judicial officers of the difficulty of refuting a claim by the Attorney-General that the release of such information would damage national security was 'quite a dangerous position'. Therefore, procedures may be needed to allow a court to be confident that appropriate scrutiny has been undertaken before the certificate is signed. One mechanism to ensure this level of accountability would be to require, in each case where a ministerial certificate is issued, the tabling in Parliament of the decision with an outline of the basis on which a claim was made. The Attorney-General (or other relevant minister) could report that a certificate was issued, an outline of the circumstances in which it was issued, its effect, and an outline of the process that the minister went through before issuing the certificate.

Proposal 8–1 As a matter of principle, ministerial certificates should not be conclusive on the question of public interest immunity. Courts should retain a discretion to inspect the material and determine how the information in question should be handled. Governments would retain the ultimate strategic decision-making power insofar as they can withdraw or amend the proceedings to avoid the disclosure of the sensitive material.

Proposal 8–2 Ministers who issue certificates that determine whether information will or will not be disclosed should be required to table in Parliament a notice stating that a certificate was issued, an outline of the circumstances in which it was issued, its effect, and an outline of the process that the Minister went through before issuing the certificate. This would apply in respect of all court proceedings, applications under freedom of information legislation, investigations by the Federal Privacy Commissioner and any other lawful demand for official information that may be denied by a ministerial certificate or similar action.

8.198 The ALRC's other Proposals concerning ministerial certificates are part of the proposed new Act dealing with the protection of classified and security sensitive information discussed in Chapter 10.

Other provisions protecting information from disclosure in court

8.199 The *Terrorism (Community Protection) Act 2003* (Vic) has as one of its purposes the protection of counter-terrorism methods from disclosure in legal proceedings.[339] The Act provides that where an issue arises relating to the disclosure of

339 *Terrorism (Community Protection) Act 2003* (Vic), s 1(e). The definition of 'legal proceedings' is taken from the *Evidence Act 1958* (Vic) and includes any civil or criminal proceeding before a court, a coronial inquest, and a royal commission. Also, under the *Evidence Act 1958* (Vic), 'court' includes a person acting judicially.

counter-terrorism information in legal proceedings[340] and a person would otherwise be entitled to require a person to disclose that information, a court may excuse the person from the requirement to disclose if satisfied that:

> (a) disclosure would prejudice the prevention, investigation or prosecution of a terrorist act or suspected terrorist act; and
>
> (b) the public interest in preserving secrecy or confidentiality outweighs the public interest in disclosure.[341]

8.200 This protection is available at all stages of a proceeding and encompasses any disclosure of information, not just the adducing of evidence. 'Disclosure' is defined to include disclosure by order, subpoena or otherwise, by the:

> (a) inspection, production or discovery of documents; and
>
> (b) giving of evidence; and
>
> (c) answering of interrogatories; and
>
> (d) provision of particulars.[342]

8.201 However, the Act does not provide blanket protection for counter-terrorism information.

> [A] case by case decision must be made about whether the public interest in protecting the information (for example, the interest in effective investigation of terrorist activity which relies on the protection of covert methods) is greater than the public interest in disclosing the information (for example in a criminal proceeding, the interests of justice served by having the defendant having access to all relevant information to defend the case). The same balancing exercise is currently required at common law, under the doctrine of public interest immunity.[343]

8.202 The Act sets out the matters to which the court must have regard in assessing the potential impact of disclosure and deciding where the balance lies, although the court is not limited to consideration of those matters. The matters include: the importance of the information in the legal proceedings; in the case of criminal proceedings whether the party seeking disclosure of the information is the defendant or the prosecutor and whether the order is to be made subject to the condition that the prosecution be stayed; the nature of the offence, cause of action or defence to which the information relates; and the likely effect of disclosure of the information and methods available to limit its

---

340 'Counter-terrorism information' is defined as 'information relating to covert methods of investigation of a terrorist act or suspected terrorist act': *Terrorism (Community Protection) Act 2003* (Vic), s 3. 'Terrorist act' is defined in s 4 of the Act.

341 Ibid, s 23(1).

342 Ibid, s 23(4).

343 Terrorism (Community Protection) Bill Explanatory Memorandum 2003 (Vic).

publication.[344] In making its decision, the court may inspect a document for which protection is being considered.[345]

Closing courts to the public

8.203 Common mechanisms for dealing with classified and security sensitive information include holding 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.[346] These types of orders are, by their nature, a departure from the general principles of open justice discussed in Chapter 7. It is possible to get a variety of orders in relation to restricting access to court proceedings, including an order making a transcript confidential and orders in relation to who may have access to the transcript, how the transcript is to be stored or the placing of documents in sealed envelopes.[347] The duration of orders prohibiting publication is an important factor. The court may prohibit publication for such time as the information that is the subject of the order is deemed to be security sensitive, any such prohibition order ceasing once the sensitivity has lapsed.

8.204 Another type of suppression order that may be considered in this context is an order suppressing the identity of any person, such as a juror, who comes into contact with classified or security sensitive information in the course of proceedings in order to prevent pressure being put on the person after the proceedings.[348]

---

344 See *Terrorism (Community Protection) Act 2003* (Vic), s 23(2) for other matters the court must consider.

345 Ibid, s 24.

346 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. It has been reported that South Australian courts made 214 suppression orders in the 2002–2003 financial year —an increase of 33 on the year before. There were 88 suppression orders in the Supreme Court, 73 in the District Court and 46 in the Magistrates Court. 'The major reason for the orders—in 125 cases—was "to prevent prejudice to the proper administration of justice." There were 19 orders to prevent the publication of details concerning the accused, victims or witnesses and 14 to prevent undue hardship to witnesses': 'More Court Suppression Orders', *The Advertiser* (Adelaide), 12 November 2003. It is not possible from the generic reason provided of preventing 'prejudice to the proper administration of justice' to deduce how many suppression orders in South Australia were made to protect classified or security sensitive information, or to protect national security. There may be some benefit in requiring courts to report, in a readily available medium, on an aggregated basis on their use of suppression orders and the basis of their issue. For example, the *Federal Court of Australia Annual Report* (2002–2003) does not contain any statistics on the use by the Federal Court of suppression orders made under the *Federal Court of Australia Act 1976* (Cth), s 50 to prevent prejudice to the security of the Commonwealth. Section 50 is discussed at [8.222]–[8.224] below.

347 B Leader, *Consultation*, By telephone, 26 August 2003. For example, in *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 1)* (Unreported, Federal Court of Australia, Lockhart J, 18 December 1989), Lockhart J ordered that ASIO security assessments 'be placed in an envelope to be sealed by the New South Wales District Registrar of the Court which shall not be opened except by leave of a judge and shall not be available for the inspection of any person'.

348 See Australian Federal Police, *Submission CSSI 13*, 18 September 2003. See also Proposal 10–10(b)(iv).

8.205 In *Scott v Scott* the House of Lords stated:

> While the broad principle is that the Courts of this country must, as between parties, administer justice in public, this principle is subject to apparent exceptions … But the exceptions are themselves the outcome of a yet more fundamental principle that the chief object of the Courts of justice must be to secure that justice is done.[349] …
>
> I think that to justify an order for hearing *in camera* it must be shown that the paramount object of securing that justice is done would really be rendered doubtful if the order were not made.[350] …
>
> [I]n very exceptional cases … where a judge finds that a portion of the trial is rendered impractical by the presence of the public, he may exclude them so far as to enable the trial to proceed. It would be impossible to enumerate or anticipate all possible contingencies, but in all cases where the public has been excluded with admitted propriety the underlying principle, as it seems to me, is that the administration of justice would be rendered impractical by their presence, whether because the case could not be effectively tried, or the parties entitled to justice would be reasonably deterred from seeking it at the hands of the court.[351]

8.206 In *McPherson v McPherson* the Privy Council stated:

> It cannot be denied that in the light of the language in *Scott v Scott* a trial of an action must be in open court. There must, however, be some limit to that, it cannot mean that all parts of a trial must be in open court … [352]

8.207 In practice, the Australian Government rarely seeks to close courts, and with some reluctance.[353] The authorities establish that, where possible, measures less drastic than a closed court should be adopted.

> Even where a court is vested with a statutory discretion to exclude the public, it would ordinarily exercise that power only in cases where lesser procedures are clearly inadequate to give the confidentiality which is seen to be necessary.[354]

8.208 The NSW Court of Appeal has commented that, rather than close a court:

> which our history and law and established principle demonstrate to be so exceptional, the court will strive to adopt other expedients, such as the placing of a matter before a court in writing so that it is conveyed to the court in public but not read out: see *R v Ealing Justices; Ex parte Weafer* (1981*)* 74 Cr App R 204 at 206.[355]

---

349 *Scott v Scott* [1913] AC 417, 437 (Viscount Haldane LC).
350 Ibid, 439 (Viscount Haldane LC).
351 Ibid, 446 (Lord Loreburn).
352 *McPherson v McPherson* [1936] AC 177, 190.
353 J Renwick, *Consultation*, Sydney, 9 September 2003.
354 *R v Tait and Bartley* (1979) 24 ALR 473, 490.
355 *Raybos Australia v Jones* (1985) 2 NSWLR 47, 54–55. See also *Attorney-General v Leveller Magazine* [1979] AC 440, 471 where 'the justices instead of sitting in private, adopted the device of allowing a piece of evidence to be written down and requiring it not to be mentioned in open court.' The piece of evidence in that case was the real name and address of a person, referred to in the hearing as 'Colonel B'.

8.209 In the UK case of *R v Socialist Worker Printers and Publishers Ltd, Ex parte Attorney-General*, Lord Widgery made it clear that the court, where it could, would prefer the use of protective orders such as suppression of the names of witnesses rather than an order for in-camera proceedings:

> [T]here is such a total and fundamental difference between the evils which flow from a court sitting in private and the evils which flow from pieces of evidence being received in the way which was followed in this case. …
>
> Where one has an order for trial in camera, all the public and all the press are evicted at one fell swoop and the entire supervision by the public is gone. Where one has a hearing which is open, but where the names of the witnesses are withheld, virtually all the desirable features of having the public present are to be seen.[356]

8.210 In *Ex parte The Queensland Law Society Incorporated*, McPherson J, on reviewing the authorities in relation to the prohibition of publication out of court of proceedings heard in public, stated:

> [A]part from specific statutory provision, the power of the court under general law to prohibit publication of proceedings conducted in open court has been recognized and does exist as an aspect of the inherent power. That does not mean that it is an unlimited power. The only inherent power that a court possesses is power to regulate its own proceedings for the purpose of administering justice; and apart from securing that purpose in proceedings before it, there is no power to prohibit publication of an accurate report of those proceedings if they are conducted in open court, as in all but exceptional cases they must be.[357]

8.211 The Law Council of Australia submitted that:

> The real problem appears to be a residual uncertainty as to when the circumstances are such as to justify the making of restricted publicity orders and the reach of such orders. For example, Nettheim identifies the issue whether an exercise of the court's inherent power can lawfully extend to bind non-parties in regard to conduct outside the court room.[358]

8.212 Section 93.2 of the *Criminal Code Act 1995* (Cth)[359] allows a judge or magistrate at any time before or during a hearing of an application or proceedings before a

---

That evidence was only to be disclosed to the court, the defendants and their legal representatives: *Attorney-General v Leveller Magazine* [1979] AC 440, 451.

356 *R v Socialist Worker Printers and Publishers Ltd, Ex parte Attorney-General* [1975] QB 637, 651–652.

357 *Ex parte The Queensland Law Society Incorporated* [1984] 1 Qd R 166, 170. The court noted that in *R v Clement* (1821) 106 ER 918, where the court had made an order prohibiting publication of the proceedings of the trial of several individuals for high treason, it had only done so because the trials of the accused followed on successive days and there existed a danger of prejudice to them if witnesses were able to read their own testimonies and that of others before giving evidence in a later trial in the series. The King's Bench had upheld the order, noting that it was made for the furtherance of justice in those proceedings and was to remain in force only during the pendency of those proceedings.

358 Law Council of Australia, *Submission CSSI 11*, 12 September 2003 citing G Nettheim, 'Open Justice and State Secrets' (1986) 10 *Adelaide Law Review* 281, 312.

359 Section 93.2 was introduced into the *Criminal Code Act 1995* (Cth) by the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth). It is set out in Appendix 3.

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.[360]

8.213 These orders are identical to those that a court can make under s 85B of the *Crimes Act 1914* (Cth).[361] 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.'[362] It is unclear what (if any) practical difference exists in the effect of the two sections.[363]

8.214 The Law Council submitted that s 93.2 of the *Criminal Code Act 1995* (Cth) and s 85B of the *Crimes Act 1914* (Cth) 'provide sufficient power to enable judges exercising federal jurisdiction to protect security sensitive information by closing proceedings in whole or part or making restrictive orders.'[364] However, the Attorney-General's Department submitted that s 85B is inadequate to protect security classified information during criminal proceedings as it does not extend to the protection of security classified information that may not relate to the defence of the Commonwealth, but may instead relate to Australia's international relations.[365]

8.215 Other provisions in Australia and overseas also allow for in-camera hearings.[366] Section 17(4) of the *Federal Court of Australia Act 1976* (Cth) provides that:

---

360 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).

361 The text of *Crimes Act 1914* (Cth), s 85B is set out in Appendix 3.

362 *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'.

363 The ALRC is expressly required to consider the operation of s 85B of the *Crimes Act 1914* (Cth) by the Terms of Reference: see p 5 above. Section 85B is set out in Appendix 3.

364 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

365 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

366 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 cer-

> The Court may order the exclusion of the public or of persons specified by the Court from a sitting of the Court where the Court is satisfied that the presence of the public or of those persons, as the case may be, would be contrary to the interests of justice.

8.216 Section 80 of the *Supreme Court Act 1970* (NSW) provides:

> Subject to any Act, the business of the Court may be conducted in the absence of the public:
>
> (a) on the hearing of an interlocutory application, except while a witness is giving oral evidence,
>
> (b) where the presence of the public will defeat the ends of justice,
>
> (c) where the business concerns the guardianship, custody or maintenance of an infant,
>
> (d) where the proceedings are not before a jury and are formal or non-contentious,
>
> (e) where the business does not involve the appearance before the Court of any person,
>
> (f) in proceedings in the Equity, Probate or Protective Division, where the Court thinks fit,
>
> (f1) in proceedings on an application under section 25 or 26 of the Summary Offences Act 1988, or
>
> (g) where the rules so provide.[367]

8.217 The *Witness Protection Act 1995* (NSW) provides that all business of the Supreme Court under Part 3 of the Act, which deals with protecting witnesses from identification, is to be conducted in the absence of the public.[368] For example, applica-

---

tain 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] (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; *Official Secrets Act 1989* (UK), s 11(4) (discussed below at [8.226]); and *Criminal Code* [RS 1985, c C–46] (Canada), s 486(1), which provides that proceedings against an accused are to be held in open court but allows the court to 'exclude any members of the public from the court room for all or part of the proceedings' where it is necessary for, among other things, 'the proper administration of justice' or to 'prevent injury to international relations or national defence or national security'. In *Canadian Broadcasting Corp v New Brunswick (Attorney General)* [1996] 3 SCR 480, [69], La Forest J stated that a judge exercising discretion to exclude media and public access under *Criminal Code* [RS 1985, c C–46] (Canada) must (a) consider available options and whether there are any other reasonable and effective alternatives available; (b) consider whether the order is limited as much as possible; and (c) weigh the importance of the objectives of the particular order and its probable effects against the importance of openness and the particular expression that will be limited in order to ensure that the positive and negative effects of the order are proportionate.

367 See also *Supreme Court Act* (NT) s 17 and *Criminal Code* (WA) s 635A(2). Counsel or a solicitor engaged in the trial or other criminal proceeding is not to be excluded under the latter section: *Criminal Code* (WA), s 635A(4).

368 *Witness Protection Act 1995* (NSW), s 16.

tions to the Supreme Court by the Commissioner of Police for a court order authorising a specified person to make a new entry in the register of births or the register of marriages in respect of a witness, or to make a new entry in the register of deaths in respect of a witness or a relative of a witness, or to issue in the witness's new identity documents of a kind previously issued to the witness, are to be heard in private.[369]

8.218 The *Terrorism (Community Protection) Act 2003* (Vic) provides that the Supreme Court must be closed to the public whenever it hears an application for a covert search warrant.[370] The purpose of this is to 'ensure that information that could jeopardise the successful conduct of the search is not made public'.[371]

8.219 The *Supreme Court Act 1986* (Vic), and the *County Court Act 1958* (Vic) allow the Supreme Court and the County Court respectively to:

(a) order that the whole or any part of a proceeding be heard in closed court; or

(b) order that only persons or classes of persons specified by it may be present during the whole or any part of a proceeding; or

(c) make an order prohibiting the publication of a report of the whole or any part of a proceeding or of any information derived from it;[372]

where in their opinion it is necessary to do so in order not to endanger the national or international security of Australia or not to prejudice the administration of justice.[373] These orders can be made in any proceeding, whether civil or criminal.[374]

8.220 Both Victorian Acts also usefully provide that an order made under these sections must be placed on the door of the courthouse or in another conspicuous place where notices are normally placed at the courthouse.[375] The concern has been expressed to the ALRC that orders made by courts to close a courtroom or to restrict the

---

369 Such applications are made under Ibid, s 15 and the court can only make such an order if it is satisfied of the criteria set out in s 17, which include that the life or safety of the person may be endangered as a result of the person being a witness.

370 *Terrorism (Community Protection) Act 2003* (Vic), s 6(2).

371 Terrorism (Community Protection) Bill Explanatory Memorandum 2003 (Vic). The Act also prohibits the publishing of any report of the proceedings for an application for a covert search warrant, or any information derived from such a proceeding or part of any report made under the Act to the Supreme Court by the person to whom the warrant was issued, unless the Supreme Court orders otherwise: *Terrorism (Community Protection) Act 2003* (Vic), s 12. However, as noted in Ch 7 at [7.33] there is a difference between hearings in camera in relation to proceedings relating to the investigative process, and hearings in camera in the context of a trial or trial proceedings.

372 *Supreme Court Act 1986* (Vic), s 18(1) and *County Court Act 1958* (Vic), s 80(1).

373 See *Supreme Court Act 1986* (Vic), s 19 and *County Court Act 1958* (Vic), s 80AA. Similar orders can also be made under the *Magistrates' Court Act 1989* (Vic), s 126, which, in addition, allows the court to 'make an order prohibiting the publication of any specified material, or any material of a specified kind, relevant to a proceeding that is pending in the Court.'

374 *Supreme Court Act 1986* (Vic), s 18(2) and *County Court Act 1958* (Vic), s 80(2).

375 *Supreme Court Act 1986* (Vic), s 18(3) and *County Court Act 1958* (Vic), s 80(3). A similar provision is also found in *Magistrates' Court Act 1989* (Vic), s 126(3).

publication of proceedings are not always properly notified to the public and the media in order to ensure compliance with them; nor are they consistently enforced by court staff. For example, the NSW Police Service submitted that:

> The NSW criminal justice system provides for such matters to be heard in camera and/or the court may issue suppression orders prohibiting the publication of certain information. However, some concerns have been raised in recent discussions with officers of the Office of the Director of Public Prosecutions that some courts are not sign posted during such hearings nor are they properly supervised after the hearing has commenced to prevent any other persons and in particular the media, from entering the court room. The matter is a question of supervision within each court jurisdiction and the availability of NSW Sheriff's officers at each court to control such access.[376]

8.221 Where legislation provides that a court may order in-camera proceedings or the making of suppression orders, in order to enhance compliance with any such order by the public and the media, the court should also take all appropriate practical steps to ensure that it is complied with by using appropriate notices, informing all relevant court staff, and so on. There also appears to be some need for the development of procedures to be followed in order to enforce compliance with such orders, and for the training of court officers in the procedures to be followed. Where in-camera hearings or suppression orders are made in order to protect classified or security sensitive information, enforcement of the orders, by ensuring that procedures are adhered to, could be a task well suited to be performed by a court security officer or case manager appointed to assist the court on these technical and security issues.[377]

8.222 Other provisions in Australian legislation also allow for orders restricting the publication of proceedings. 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'.[378]

8.223 In *Australian Broadcasting Commission v Parish*, parties appealed against the order of a trial judge refusing an application under s 50 for an order forbidding or restricting the publication of certain parts of an agreement specified as confidential, and their appeal was upheld. Franki J held that the trial judge had acted on an incorrect principle by taking the view that the 'possibility of the public not being able to appreciate adequately the nature and course of the proceedings and the issues to be

---

376 NSW Police, *Submission CSSI 7*, 29 August 2003. A concern was raised in consultation that breaches of such orders can also be difficult to prosecute as the prosecution has not always been able to prove non-revocation of such an order or that the order was still in force: Director of Public Prosecutions for Victoria, *Consultation*, Melbourne, 29 August 2003.

377 See discussion on court security officers appointed in the US under CIPA at [8.73] and Proposal 10–36.

378 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; *Nuclear Non-Proliferation (Safeguards) Act 1987* (Cth), s 40; *Criminal Code* (WA), s 635A(2)(b) and (c); and *Criminal Records Act 1991* (NSW), 16(2).

determined outweighed the necessity of doing justice between the parties.'[379] Franki J stated that:

> I do not see how justice can be done between the parties when a document is made public, not for the purpose of the judge coming to the correct conclusion, but merely for the purpose of enabling the public to perhaps more fully appreciate the nature and course of the proceedings by which issues are to be determined where this course of action will weaken the negotiating strength of one of the parties and may even result in the parties having to reconsider adherence to the agreement.[380]

8.224 Franki J noted that the provisions of s 17(4) (allowing for closed courts) and s 50 (restrictions on publication) of the *Federal Court of Australia Act 1976* had been used on a number of occasions in matters under the *Trade Practices Act 1974* (Cth). He noted that, by providing those specific powers, the Parliament intended that, while the court would have regard to the desirability of conducting proceedings in open court, it would make orders under those sections to ensure that a party would not be seriously prejudiced.[381]

> Of course, if the trial judge decides when the proceedings have gone further, that protection is no longer warranted he can remove the protection effected under s 50 and the material which was not available to the public would then become open to the public.[382]

8.225 The *Migration Act 1958* (Cth) also authorises the Federal Court and the Federal Magistrates Court, on application by the Minister, to make non-disclosure orders to protect confidential information disclosed to them. These orders include:

> (a) an order that some or all of the members of the public are to be excluded during the whole or a part of the hearing of the substantive proceedings;
>
> (b) an order that no report of the whole of, or a specified part of, or relating to, the substantive proceedings is to be published; or
>
> (c) an order for ensuring that no person, without the consent of the Federal Court or the Federal Magistrates Court, has access to a file or record of the Federal Court or the Federal Magistrates Court that contains the information.[383]

8.226 In the United Kingdom, s 8(4) of the *Official Secrets Act 1920* (UK) enables the prosecution to apply for all or any part of the public to be excluded during any part of proceedings against a person for an offence under the Act 'on the ground that the publication of any evidence to be given or any statement to be made in the course of the proceedings would be prejudicial to the national safety'. Section 11(4) of the *Offi-*

---

379 *Australian Broadcasting Commission v Parish* (1980) 29 ALR 228, 245.
380 Ibid, 245.
381 Ibid, 245, 246.
382 Ibid, 246.
383 *Migration Act 1958* (Cth), s 503B(2), introduced by the *Migration Legislation Amendment (Protected Information) Bill 2003* on 15 July 2003. Other orders that the Federal Court or Federal Magistrates Court can make are discussed in Ch 9 at [9.53] below under the heading 'Immigration Cases'.

cial Secrets Act 1989 (UK) applies the earlier provisions to the 1989 Act. The *Crown Court Rules 1982* (UK) set out the procedure to be followed 'when a prosecutor or a defendant intends to apply for an order that all or part of a trial be held in camera for reasons of national security or for the protection of the identity of a witness or any other person'.[384] The procedure entails the giving of notice not less than seven days before a trial is expected to begin[385] and the displaying of the notice 'in a prominent place within the precincts of the Court.'[386] The application itself is heard in camera unless the Court otherwise orders.[387] It is to be made:

> after the defendant has been arraigned but before the jury has been sworn and, if such an order is made, the trial shall be adjourned until whichever of the following shall be appropriate:
>
> (a) 24 hours after the making of the order, where no application for leave to appeal from the order is made, or
>
> (b) after the determination of an application for leave to appeal, where the application is dismissed, or
>
> (c) after the determination of the appeal, where leave to appeal is granted.[388]

8.227 In the UK, an aggrieved person, if granted leave, may appeal to the Court of Appeal against:

> (b) any order restricting the access of the public to the whole or any part of a trial on indictment or to any proceedings ancillary to such a trial; and
>
> (c) any order restricting the publication of any report of the whole or any part of a trial on indictment or any such ancillary proceedings; and the decision of the Court of Appeal shall be final.[389]

8.228 Bans on publication are also available under the *Criminal Code* (Canada).[390] In proceedings against an accused for terrorism offences (as well as specified offences under the *Security of Information Act*),[391] a court may make an order directing that the identity of a 'justice system participant' who is involved in the proceedings, or any information that could disclose their identity, 'shall not be published in any document or broadcast in any way, if the court is satisfied that the order is necessary for the

---

384 *Crown Court Rules 1982* (UK), Rule 24A(1).
385 Ibid, Rule 24A(1).
386 Ibid, Rule 24A(2).
387 Ibid, Rule 24A(3).
388 Ibid, Rule 24A(3).
389 *Criminal Justice Act 1988 (C.33)* (UK), s 159(1)(b) and (c). On the hearing of such an appeal, the Court of Appeal has power to stay the proceedings in any other court until the appeal is disposed of; and to confirm, reverse or vary the order complained of: *Criminal Justice Act 1988 (C.33)* (UK), s 159(5).
390 See *Criminal Code* [RS 1985, c C–46] (Canada), s 486 (4.1) and (4.11).
391 [RS 1985, c0-5].

proper administration of justice'.[392] The court may hold a hearing to determine whether such an order should be made, and the hearing may be in private.[393] An order may be made subject to any conditions that the court thinks fit.[394] The *Criminal Code* sets out the factors that the court must consider in deciding whether to make such an order. These include, among others, the right to a fair and public hearing, whether there is a real and substantial risk that the justice system participant would suffer significant harm if their identity were disclosed, and the impact of the proposed order on the freedom of expression of those affected by it.[395]

8.229 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, and defence counsel were given access at that time.[396] The proceedings involved some wide-ranging exploration of the Crown case by defence counsel. The fact that the proceedings were held in camera enabled questions to be put to Crown witnesses unconstrained by any risk of causing further security breaches.[397] However, Gray J required Lappas's trial to be conducted in open court as far as possible. Accordingly, the Crown opening was conducted in two stages. First, there was a general outline of the case in open court. Following this, an order was made that members of the public vacate the court and the Crown then made further detailed opening statements, referring to the evidence that would be tendered in camera. Similarly, parts of the evidence of some witnesses were led in open court, and other parts were led in camera. The view has been expressed that:

> The resulting procedure was perfectly adequate to give anyone observing the trial an understanding of what was alleged and the manner in which it was to be proved. … There should have been no loss of public confidence in the criminal justice system from the limited closures of the Court, the necessity of which would have been perfectly evident to anyone following the proceedings.
>
> There would appear to be no call for any reform of the law concerning the extent to which in camera hearings are used.[398]

8.230 Another example was the appeal proceedings in *Grant v Headland* in the ACT Supreme Court.[399] The appellant was a probationary trainee with ASIO who appealed his conviction and sentence for a breach of s 79(3) of the *Crimes Act 1914* (Cth) for attempting to communicate prescribed information to a person not authorised to

---

392 *Criminal Code* [RS 1985, c C–46] (Canada), s 486 (4.1). If such an order is made, the publication or broadcast of the contents of the application for such an order are also prohibited: *Criminal Code* [RS 1985, c C–46] (Canada): s 486(4.9)(a).

393 *Criminal Code* [RS 1985, c C–46] (Canada), s 486(4.6). If the order is made, the publication or broadcast of the contents of any evidence taken, information given or submissions made at such a hearing is also prohibited: *Criminal Code* [RS 1985, c C–46] (Canada), s 486(4.9)(b).

394 *Criminal Code* [RS 1985, c C–46] (Canada), s 486(4.8).

395 See Ibid, s 486(4.7).

396 Department of the Parliamentary Library Information and Research Services, *Bills Digest No 117: Criminal Code Amendment (Espionage and Related Offences) Bill 2002*, Appendix.

397 Advisory Committee member, *Correspondence*, 18 September 2003.

398 Ibid.

399 *Grant v Headland* (1977) 17 ACTR 29.

receive it.[400] Smithers J noted that, although the magistrate had not found it necessary to assess the security quality of the information in question, the appeal court must do so. In this regard, he had the assistance of security experts called upon by the Crown. Smithers J stated:

> This appeal was heard in camera because it was considered inexpedient in the interests of the defence of the Commonwealth to do otherwise. In addition counsel for the appellant would have found himself hampered in cross-examination and otherwise if he had not been free of security considerations in his conduct of the case.
>
> Throughout I have been aware that justice should be done in public, and matters heard in camera only for compelling reasons.[401]

8.231 The committal proceedings in 1994 against George Sadil, an ASIO officer, for several offences under the *Crimes Act 1914* (Cth) relating to espionage and the disclosure of official secrets were held in both closed court and open court.[402]

8.232 One Australian commentator has suggested 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.[403]

8.233 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.[404]

---

400 'Prescribed information' is relevantly defined in *Crimes Act 1914* (Cth), s 79(1)(b) in these terms: 'information is prescribed information in relation to a person if the person has it in his possession and control and … he has obtained it owing to his position as a person … who is or has been a Commonwealth officer … and by reason of … the circumstances under which it is entrusted to him … or for any other reason, it is his duty to keep it a secret.'

401 *Grant v Headland* (1977) 17 ACTR 29, 34.

402 Commonwealth Director of Public Prosecutions, *Consultation*, By telephone, 3 November 2003. Sadil was committed for trial in March 1994. On reviewing the evidence, the Director of Public Prosecutions decided not to proceed with the more serious espionage-related charges. Sadil pleaded guilty in December 1994 to 13 summary charges of removing ASIO documents contrary to his duty. He was sentenced to three months' jail, and released on a 12 month good behaviour bond: <www.asio.gov.au/About/Timeline/Content/main.htm>.

403 H Selby, 'A Middle Way to Countering Terror', *The Canberra Times*, 11.

404 C Maher, 'The Right to a Fair Trial in Criminal Cases Involving the Introduction of Classified Information' (1988) 120 *Military Law Review* 83, 125.

8.234 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.[405] 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.[406]

> 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'.[407]

8.235 There appears to be some merit in the US approach requiring the issue of specific findings of fact justifying the closure of criminal proceedings. Such an approach could legitimately be extended to criminal and civil proceedings in Australia. In this regard, see the conclusions in Chapter 10 at [10.84], and Proposal 10–20.

Closing tribunals to the public

8.236 Non-curial tribunals may also hold hearings in camera and issue suppression orders. Australian tribunals with these powers (to varying degrees) include the Administrative Appeals Tribunal (AAT), the Federal Police Disciplinary Tribunal, the Migration Review Tribunal and the Refugee Review Tribunal, the Administrative Decisions Tribunal (NSW), and the Victorian Civil and Administrative Tribunal. In some circumstances the tribunals have discretion to hold closed hearings; while in other circumstances they are required by legislation to hold closed hearings.

8.237 Section 39A of the *Administrative Appeals Tribunal Act 1975* (Cth) (AAT Act) sets out the procedure for certain hearings in the AAT's Security Appeals Division dealing with applications for review of security assessments. Section 39A(5) states that those proceedings are to be in private and that the tribunal is to determine who may be present at the hearing. In relation to proceedings before the Security Appeals Division to which s 39A applies, the AAT may give directions prohibiting or restricting the publication of:

> (a) evidence given before the Tribunal; or
>
> (b) the names and addresses of witnesses before the Tribunal; or
>
> (c) matters contained in documents lodged with the Tribunal or received in evidence by the Tribunal; or

---

405 The text of the First Amendment is set out in Appendix 3.

406 *Globe Newspaper Co v Superior Court* 457 US 596 (1982); *United States v Cojab* 996 F 2d 1404 (2nd Cir, 1993).

407 *Press-Enterprise Co v Superior Court (Press-Enterprise I)* 464 US 501 (1984); *Press-Enterprise Co 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> at Winter 2002.

(d) the whole or any part of its findings on the review.[408]

8.238 Section 35(2) of the AAT Act sets out the various orders that the AAT can make in divisions other than the Security Appeals Division where it is satisfied that it is desirable to do so because of the confidential nature of any evidence or for any other reason.[409]

8.239 The view was expressed to the ALRC that accidental disclosure risk is high in a court, but higher in the AAT because there is more sensitive material.[410] This calls for internal tribunal procedures to be adequate in relation to the protection of such material.

8.240 Where the Federal Police Disciplinary 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, it 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.[411]

8.241 Where the Migration Review Tribunal (MRT) is satisfied that it is in the public interest to do so, it may 'direct that particular oral evidence, or oral evidence for the purposes of a particular review, is to be taken in private.'[412] Where it makes such a direction, it may give directions as to the persons who may be present when the oral evidence is given.[413] The MRT can also restrict publication of certain matters. Section 378(1) of the *Migration Act 1958* (Cth) provides that:

---

408 *Administrative Appeals Tribunal Act 1975* (Cth), s 35AA.

409 These include directing that a hearing or part of a hearing take place in private; the giving of directions prohibiting or restricting the publication of the names and addresses of witnesses, or of evidence given before the Tribunal, whether in public or in private, or of matters contained in documents lodged with the Tribunal or received in evidence by the AAT: Ibid, s 35(2)(a), (aa) and (b).

410 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003. See Ch 10 at [10.119].

411 *Complaints (Australian Federal Police) Act 1981* (Cth), s 74(2). See also the *Administrative Decisions Tribunal Act 1997* (NSW), s 75(2), and the *Victorian Civil and Administrative Tribunal Act 1998* (Vic), Part 8, Sch 1, s 29D(1) and 2(b), which provides an exemption if a document affects national security, defence or international relations. See discussion on freedom of information in Ch 3.

412 *Migration Act 1958* (Cth), s 365(2). The MRT may also direct that evidence be taken in private where it is satisfied that it is impracticable to take particular oral evidence in public: *Migration Act 1958* (Cth), s 365(3).

413 *Migration Act 1958* (Cth), s 365(4).

> Where the Tribunal is satisfied, in relation to a review, that it is in the public interest that:
>
> (a) any evidence given before the Tribunal;
>
> (b) any information given to the Tribunal; or
>
> (c) the contents of any document produced to the Tribunal;
>
> should not be published, or should not be published except in a particular manner and to particular persons, the Tribunal may give a written direction accordingly.[414]

8.242 In contrast, reviews before the Refugee Review Tribunal are always to be held in private. The *Migration Act 1958* (Cth) provides that the hearing of an application for review by the RRT must be in private.[415] The RRT may also restrict publication or disclosure of certain matters.[416]

8.243 In the UK, the Investigatory Powers Tribunal (UK) was established to investigate complaints about the intelligence services or relating to the interception of communications. The Tribunal has discretion as to whether or not to hold an oral hearing but Rule 9(6) of the Investigatory Powers Tribunal Rules 2000 provides that 'the Tribunal's proceedings, including any oral hearings, shall be conducted in private.'[417] Since its inception, not a single complaint has been upheld, and the system has been criticised for being unduly secretive.[418]

8.244 Most Australian parliamentary committees may hear testimony in camera.[419] The *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters* 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

---

414 The penalty for contravening such a direction is imprisonment for two years: Ibid, 378(3). A direction under the section does not excuse the MRT from its obligations under *Migration Act 1958* (Cth), s 368 to record its decisions.

415 *Migration Act 1958* (Cth), s 429.

416 Ibid, s 440 provides that if the RRT is satisfied in relation to a review that it is in the public interest that any evidence, information or contents of any document given to it 'should not be published or otherwise disclosed except in a particular manner and to particular persons', the RRT may give a written direction accordingly. The penalty for contravening such a direction is imprisonment for two years: *Migration Act 1958* (Cth), s 440(3). Such a direction does not excuse the RRT from its obligation under *Migration Act 1958* (Cth), s 430 to record its decisions.

417 See *In the Investigatory Powers Tribunal In Camera—In the Matter of Applications Nos IPT/01/62 and IPT/01/77—Draft Rulings of the Commission on Preliminary Issues of Law*, 23 January 2003 in relation to the scope of Rule 9(6).

418 S Miller and R Norton-Taylor, *At Last, a Foot in the Door*, The Guardian, <www.guardian.co.uk/freedom/Story/0,2763,880980,00.html> at 23 January 2003. See further discussion below on the Investigatory Powers Tribunal under the heading 'Tribunals closed to a party–Overseas' in Ch 9 at [9.49]–[9.52].

419 Commonwealth of Australia, *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters*, 10, citing Senate Parliamentary Privilege Resolutions (1988), rules 1.7, 1.8 and 2.7.

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.[420]

8.245 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.[421] Other protections may also be extended to witnesses, such as not publishing names in transcripts of evidence or in reports.[422] 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.[423]

Consultations and submissions

8.246 In relation to the closure of courts in general, the NSW Law Society submitted that:

> It should continue to be a fundamental principle that any judicial proceeding be 'open to the public and may be freely reported'. Any departure from this principle should be only to the minimum extent necessary to protect the public interest (including for reasons of national security) or confidentiality where this is necessary on good and established grounds. Mandatory statutory restrictions should be imposed only in the most extraordinary and clearly defined situations. The statutory response should be to equip judicial officers and other decision makers with discretionary powers to impose appropriate restrictions required for the individual circumstances of each situation.[424]

8.247 The Australian Press Council submitted that it was opposed to the use of in-camera proceedings for the purposes of protecting security sensitive information.

> This mechanism is already used to protect the identities of witnesses and parties in certain proceedings, particularly where juveniles are involved. It is, however, exceptional and the exclusion of the public from judicial proceedings is widely regarded as antithetical to justice and even unconstitutional.
>
> *In camera* proceedings should only be used for the purpose of protecting security sensitive information *only* where there is no reasonable alternative means of doing so.[425] [citations omitted]

8.248 The Australian Press Council also stated that:

> An aspect of the restrictions set down in section 93.2 which is of concern is that the circumstances in which they may be employed are not sufficiently defined or limited. The section merely requires that the court is satisfied that any restrictions imposed are

420 Ibid, 10.
421 H Evans (ed), *Odger's Australian Senate Practice Tenth Edition*, Commonwealth of Australia, <www.aph.gov.au/senate/pubs/html/httoc.htm>, 438.
422 Ibid, 438.
423 Ibid, 420.
424 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.
425 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

> in the interest of the security or defence of the Commonwealth. Section 90.1 of the *Criminal Code* extends the definition of security or defence to include the 'operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'. Thus the scope of s 93.2 is potentially extremely broad.[426]

8.249 The Australian Press Council submitted that s 93 of the *Criminal Code*, and any statutes or rules of court which allow the hearing of proceedings in camera, be amended to insert a threshold test to be satisfied before public access to proceedings can be removed. This test would require judicial officers to assess the risk to Commonwealth security posed by the disclosure of security sensitive information and weigh this against the public interest in hearing the matter in public, before excluding any members of the public from the court or denying public access to court documents.[427]

> Section 93.2 gives judicial officers the power to prevent members of the public from viewing court documents such as exhibits and affidavits. This mechanism may prevent journalists from adequately understanding or reporting on court proceedings. If, after determining that the need to protect security sensitive information outweighs the public interest in having the documents accessible to the public, a judicial officer restricts access to court documents, alternative documents should be made available to the media which provide a filtered or summarised version of the documents containing the security sensitive information, thus enabling the public to comprehend the nature of the issues in dispute without jeopardising security.[428]

8.250 In relation to the closure of Royal Commissions, the Australian Press Council submitted that:

> Royal Commissions are often concerned with scrutinising government administration and policy and may result in legislative amendment. Arguably, the public interest in having proceedings open to the public and the media is greater with regard to Royal Commissions than it is in ordinary civil or criminal proceedings. At minimum, it would be appropriate if Royal Commissions were required to apply tests which balance the danger of disclosing security sensitive information against the public interest in having that information in the public arena. Royal Commissions should also be required to allow the media to make representations as to whether or not proceedings should be heard *in camera*.[429]

8.251 In BP 8, the ALRC asked what safeguards, if any, should be available in the case of closed proceedings to protect classified and security sensitive information, the rights of the parties and the public.[430] HREOC submitted that safeguards on the use of closed hearings should:

- reflect the requirement that the exclusion of the public be 'necessary in a democratic society';

---

426 Ibid.
427 Ibid.
428 Ibid.
429 Ibid.
430 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 26.

- reflect the requirement of proportionality;
- ensure that clear reasons for not providing a public trial are given and recorded.[431]

8.252 The ALRC also asked whether, prior to closing a court to lead classified or security sensitive information, there should be a review of the classification decisions relating to the evidence to be adduced, and who should be responsible for such a review.[432] Two views were put forward in this regard, although they may be reconciled as they in effect address two different issues. The first issue is whether a classification status should ever be determinative on the issue of closure, and the second issue is whether, in any event, a review of a classification decision should be undertaken and by whom. The NSW Law Society submitted that:

> Any decision to close a court or a tribunal should not be based on a classification given by the person who may have generated or actioned that information under the normal Protective Security Procedures but rather by the presiding judicial officer or other decision maker that such closure is necessary because of the nature and content of the [in]formation.[433]

8.253 The Australian Press Council expressed a similar view:

> [B]efore a court grants an application for proceedings to be heard *in camera*, judicial officers should be required to assess the level of risk associated with releasing the information into the public domain. A security classification in itself should not be regarded as sufficient to warrant closing the court while evidence concerning sensitive information is being given. The agency seeking to protect the information must be required to satisfy the judicial officer that the information has the potential to cause significant damage to Australia's interests. Presumably, this would necessitate the judicial officer being given an opportunity to examine any documents which contain the sensitive information. Having conducted an assessment of the security risk associated with the information, the judicial officer should then be required to balance this risk against the public interest in having the information in the public arena. Only if these tests are satisfied should the matter proceed *in camera*.[434]

8.254 The view was also expressed that, in order to address any problems associated with the over-classification of information, there should be a review of the classification status of the material to be adduced in evidence and that:

---

431 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003. In relation to the latter requirement, HREOC referred to the case of *Estrella v Uruguay*, Communication No 74/1980 (17 July 1980), UN Doc Supp No 40 (A/38/40) at 150, in respect of which the Human Rights Committee found that a trial in camera violates Art 14(1) of the ICCPR if the State fails to provide a reason for not providing a public trial.

432 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 27.

433 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003. Similarly, the view was expressed that, if you rely on the content of the information to justify closure, the classification label becomes just one factor to be considered: J Renwick, *Consultation*, Sydney, 9 September 2003.

434 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

> The review procedure should be made by an ad-hoc committee of lawyers, ombudsmen, retired judges and magistrates. Retired intelligence agents may also be a suitable addition to the committee. Current intelligence agencies should be able to make submissions to the committee on the classification process.[435]

8.255 Closing courts to the public also raises the issue of whether a transcript should be made of the closed proceedings, and who should be able to access it (and under what conditions).[436] Submissions on this point varied, though most were in favour of transcripts being made of closed proceedings. The NSW Law Society submitted that:

> Whether a transcript is made; if so who may have access to it; the duration, extent and review mechanisms of any restrictions which may be imposed and the extent of any media access to information, should be under the control and consideration of the presiding judicial officer or other decision maker in the event it is decided that any closure of proceedings is required.[437]

8.256 The view of the NSW Law Society encompasses the possibility that a court could order that no transcript be made of a particular proceeding closed to the public.

8.257 The Attorney-General's Department submission appears to have been premised on the basis that full transcripts should be made of closed proceedings, but that access to them should be limited:

> Transcripts of closed proceedings during which security classified information is at issue should be sealed and only be available to the court and the parties on appeal. There is little point in protecting information during proceedings only to disclose it to the public by making transcripts available.
>
> Any transcripts of court proceedings that contain security classified information must be protected to the minimum standards specified in the PSM.[438] It would not be inappropriate to make transcripts available to counsel representing the parties so as to assist in the appeal process.[439]

8.258 Another submission expressed the view that there should be at least two, and possibly three, versions of the transcript of a closed proceeding. One version would be a complete and unedited transcript to be kept for possible appeal proceedings. The second version would be an edited transcript for access by the public. In exceptional circumstances, a third version of the transcript should be produced for certain lawyers, to assist them in the preparation of like cases.[440]

8.259 Victoria Legal Aid submitted that records of closed proceedings must be maintained for future reference—for example, by a court or tribunal conducting a review of

---

435 J Söderblom, *Submission CSSI 5*, 25 August 2003.

436 See Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 28.

437 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

438 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000)

439 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003 (citations omitted).

440 J Söderblom, *Submission CSSI 5*, 25 August 2003.

the proceedings.[441] The Australian Press Council also submitted that in-camera proceedings should be recorded and copies of all evidence should be retained.

> Apart from the benefit of facilitating any appeal against determination made in these circumstances, such recordings may be made available to journalists or other researchers if there is any significant alteration in Australia's foreign relations or security situation. Such recordings would also be invaluable for the purposes of historical research, if made public several decades later. There is no convincing reason for failing to record *in camera* proceedings.[442]

8.260 In BP 8, the ALRC asked whether the media or other public interest bodies should be given the right in all, or any class of, proceedings to intervene on the issue of the possible closure of, or restriction of access to or reporting of, proceedings.[443]

8.261 The Attorney-General's Department submitted that it was not necessary 'to grant any additional right to the media or public interest bodies to intervene on the question of the possible closure of or restriction of access to or reporting of proceedings where security classified information [is] at risk of disclosure.'[444] In contrast, the Press Council submitted that s 93 of the *Criminal* Code and any other statute or rule of court allowing the holding of hearings in camera, should be amended to provide that:

> Before excluding members of the public from the court or denying public access to court documents judicial officers must give media representatives an opportunity to make submissions as to whether the court should be closed.[445]

8.262 The Press Council submitted that courts should be required to give notice of their intention to close proceedings in order to facilitate any objection and that it would be appropriate for legislation to make it mandatory for courts to give such notice.[446] The Press Council also submitted that it would consider whether it was appropriate to formulate voluntary principles to guide journalists who are considering the publication of security sensitive information.

> Assuming that members of the press are not excluded from proceedings in which security sensitive information is disclosed, there is a need to consider the extent to which the media has a duty to refrain from publishing that information or to self censor where disclosure would damage Australia's security or defence. Ideally, the media should be able to publish the details of any proceedings which are relevant to an issue of public interest. However, the reckless publication of security sensitive information might reasonably be expected to result in a greater tendency of the courts to hear evidence *in camera* or to issue suppression orders preventing publication. Clearly, such restrictions would not be conducive to either a free press or transparent

---

441 Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003.

442 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

443 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 31.

444 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

445 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

446 Ibid. Commercial Television Australia also indicated that they would support the proposition that courts be required to give notice to the media before closing courts in criminal proceedings: Commercial Television Australia, *Consultation*, Sydney, 11 September 2003.

> government. It may be preferable for media representatives to themselves formulate ethical principles for the use of security sensitive information which could assist journalists in exercising their discretion to publish. Such voluntary principles may generate confidence that media representatives will deal responsibly with security sensitive information, thereby reducing the incentive for excessively restrictive legislation.[447]

8.263 In a similar vein, Commercial Television Australia told the ALRC that journalists have voluntary codes of conduct which currently deal with privacy issues but do not cover the treatment of national security information.[448]

8.264 The ALRC's preliminary views and Proposals on these issues are discussed in detail in Chapter 10. See [10.102].

Appeal mechanisms

8.265 It is common for there to be appeal mechanisms from any orders requiring disclosure of classified or security sensitive information so that, for example, a party who unsuccessfully applies for an order to close the court to the public or for a suppression order can appeal that order.[449] In order for the appeal process to be meaningful, the information must be protected from disclosure until the appeal is determined. This may mean that in some circumstances the proceedings would have to be stayed or adjourned once an appeal was instituted until the conclusion of the appeal process. If, for example, a party made an unsuccessful application to close a court to protect sensitive information and lodged an appeal in relation to that decision, the information would become public (in the absence of a stay of the proceedings) and any damage to national security or similar interests would be difficult to remedy. CIPA, for example, provides for interlocutory appeals by the United States Government to:

> a court of appeals from a decision or order of a district court in a criminal case authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information.[450]

8.266 Appeal mechanisms may also be available from other orders relating to the use of classified and security sensitive information. For example, as discussed in [8.227] above, in the UK, a person, if granted leave, may go to the Court of Appeal in relation to an order restricting access to a trial on indictment or an order restricting the reporting of such a trial. In most circumstances, appeals in relation to an order of the court restricting access to information may not compel special procedures such as a stay of the proceedings, or need for a determination of the appeal prior to the hearing proceeding. The exception would appear to be where parties in the same proceedings are, by court order, given different access to classified or security sensitive information. An

---

447 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

448 Commercial Television Australia, *Consultation*, Sydney, 11 September 2003.

449 Australian Federal Police, *Submission CSSI 13*, 18 September 2003. See too discussion on *Australian Broadcasting Commission v Parish* (1980) 29 ALR 228, at [8.223]–[8.224].

450 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 7(a).

appeal from an order made by a court restricting access to a party to material which has been used in the proceedings and to which other parties have been given a higher degree of access, should normally be determined prior to the final hearing, in order to maximise the appealing party's opportunity of receiving a fair hearing in the principal action.

8.267 Introducing appeal mechanisms for all applications to protect information also raises the prospect of delays in hearings involving classified and security sensitive information. These delays could be legitimately occasioned in cases where a party institutes an appeal in good faith. However, this could arise as a result of a party's decision to engage in tactical methods to delay or frustrate the proceedings. CIPA deals with the issue of delay by introducing strict deadlines in relation to the hearing and determination of an interlocutory appeal under the Act, whether it is heard prior to or during a trial:

> An appeal taken … either before or during trial shall be expedited by the court of appeals. Prior to trial, an appeal shall be taken within ten days after the decision or order appealed from and the trial shall not commence until the appeal is resolved. If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved and the court of appeals (1) shall hear argument on such appeal within four days of the adjournment of the trial, (2) may dispense with written briefs other than the supporting materials previously submitted to the trial court, (3) shall render its decision within four days of argument on appeal, and (4) may dispense with the issuance of a written opinion in rendering its decision. Such appeal decision shall not affect the right of the defendant, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.[451]

8.268 In Canada, orders made by a judge under the *Canada Evidence Act* authorising disclosure of sensitive information or authorising alternatives to full disclosure or prohibiting disclosure can be appealed to the Federal Court of Appeal within a defined time limit.[452]

8.269 The ALRC is attracted to the idea that time limits should be imposed on the hearing of appeals. However, the detail should be left to each of the courts to deal with in their respective rules. The ALRC's proposals in relation to appeal mechanisms appear in Chapter 10. See Proposals 10–29 and 10–30.

Prosecution guidelines

8.270 In the US, CIPA requires the 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

451 Ibid, s 7(b).

452 See *Canada Evidence Act* [RS 1985, c C–5], s 38.09. See also fn 185 above.

General, there is a possibility that classified information will be revealed'.[453] 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':[454]

> (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.[455]

8.271 As internal policy of the US Department of Justice, the *Guidelines* do not create enforceable rights for the benefit of defendants.[456] A decision by the Department not to prosecute pursuant to the *Guidelines* must be accompanied by written findings detailing the reasons for the decision.[457] The findings must 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.[458]

8.272 In Australia, the Commonwealth Director of Public Prosecutions' (CDPP) Statement on Prosecution Disclosure provides that an investigating agency[459] must provide

---

453 *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.

454 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.

455 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.

456 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.

457 *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 12(b).

458 Ibid, s 12(b).

459 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/prosecutions/disclosure/>, A2.

the CDPP with a schedule of potentially disclosable material which it considers may be immune from disclosure to the defence on public interest grounds, together with the reasons supporting such a conclusion.[460] Examples of such material include:

> (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; …[461]

8.273 In exceptional circumstances, the existence of this material should be revealed to the prosecutor separately and directly where the investigating agency considers that particular material is so sensitive that it should not be entered on the schedule.[462]

8.274 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.[463]

8.275 Where a claim for public interest immunity is made but fails, the CDPP:

> 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.[464]

8.276 The Statement on Prosecution Disclosure appears to be based on the premise that the options available to the prosecution and the investigating agency are full disclosure of the sensitive material to the defence or the making of a public interest immunity claim to prevent disclosure. Court-approved alternatives to full disclosure, such as redaction or the substitution of unclassified information for classified information, are not raised.

---

460 Ibid, F7.
461 Ibid, F7.
462 Ibid, F8.
463 Ibid, F11.
464 Ibid, F12.

8.277 The prosecution also has an obligation to disclose to the defence matters affecting the credibility or reliability of prosecution witnesses.[465] Where the identity of a witness is the subject of a claim for public interest immunity, the question arises about how the prosecution can discharge its obligations in this regard without revealing the witness's identity.[466]

8.278 The submission of the Office of the Director of Public Prosecutions of Western Australia indicates that the issue of protecting security sensitive information has never arisen in WA.[467] The Statement of Prosecution Policy and Guidelines for the WA DPP (the WA Guidelines) provides that:

> A prosecutor may withhold or delay disclosure of specific material where the prosecutor is of opinion that, in the public interest, the material should be immune from disclosure.[468]

8.279 Some of the factors to be considered by a prosecutor in making such a decision include where 'withholding is necessary to preserve the identity of an informant' and 'the material relates to national or State security'.[469] The WA Guidelines also provide:

> Where the prosecutor declines to disclose material, or alternatively delays disclosure of material, the prosecutor should advise the defence that material has been withheld and claim an immunity against disclosure in respect of that material.
>
> If a dispute arises as to the claim for immunity, the matter should be submitted to the court for resolution prior to trial.
>
> Where the circumstances require, a prosecutor may seek an undertaking that the material will not be disclosed to parties other than the accused's legal advisers and the accused.[470]

---

465 Ibid, Section D.

466 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> at 1 September 2002. Lindh later entered into a plea agreement.

467 Director of Public Prosecutions for Western Australia, *Submission CSSI 6*, 28 August 2003.

468 Director of Public Prosecutions for Western Australia, *Director of Public Prosecutions Act 1991—Statement of Prosecution Policy and Guidelines*, <www.dpp.wa.gov.au/content/PolicyProc.pdf>, Appendix 2(6).

469 Ibid, Appendix 2(7)(b), 2(7)(j).

470 Ibid, Appendix 2(8)–(10). The Office of the Director of Public Prosecutions is also subject to statutory disclosure requirements imposed by *Criminal Code* (WA), s 611B and *Justices Act 1902* (WA), s 103, which would override the obligations in the WA Guidelines in the event of a conflict between the two. The Director of Public Prosecutions for Western Australia has noted that the prosecution may be required, pursuant to the statutory obligations, to disclose material that contains classified or security sensitive information to the defence, and that consideration needs to be given to the methods available to prevent such disclosure: Director of Public Prosecutions for Western Australia, *Submission CSSI 6*, 28 August 2003.

8.280 The Australian Attorney-General's Legal Service Directions[471] specify that legal work is tied to the Australian Government Solicitor and the Attorney-General's Department if it involves national security issues. However, the tying of national security work is not intended to affect, among other things, the role of the Director of Public Prosecutions or the statutory rights conferred on agencies concerning the conduct of their legal affairs.[472] The Directions cover public interest immunity claims.[473]

8.281 The Directions on the Australian Government's obligation to act as a 'model litigant' require it to act fairly and honestly, in handling claims and litigation brought by or against the Commonwealth or an agency,[474] although the duty may extend beyond merely acting honestly and in accordance with the law and court rules.[475] Obligations of the Australian Government include avoiding undue delay, endeavouring to avoid litigation where possible, acting consistently, not requiring the other party to prove a matter which the Government or its agency knows to be true, not contesting liability if the Government or its agency knows that the dispute is really about quantum, not relying on technical defences when no prejudice has been suffered, and not undertaking and pursuing appeals unless it believes that it has reasonable prospects of success or the appeal is otherwise justified in the public interest.[476] The obligation does not preclude the Australian Government and its agencies from acting firmly to protect their interests.[477]

8.282 In the UK, the Code for Crown Prosecutors, issued by the Director of Public Prosecutions under s 10 of the *Prosecution of Offences Act 1985* (UK), sets out the basic principles Crown Prosecutors should follow when they make case decisions. In considering whether the public interest is served by a prosecution, the Code sets out some public interest factors in favour of prosecution, and some public interest factors against prosecution. One of the public interest factors against prosecution mentioned is that 'a prosecution is less likely to be needed if … details may be made public that could harm sources of information, international relations or national security.'[478]

Consultations and submissions

8.283 In BP 8, the ALRC asked whether guidelines should be developed for the disclosure, withholding and use of classified and security sensitive information in

---

471 Issued by the Attorney-General of Australia pursuant to s 55ZF of the *Judiciary Act 1903* (Cth) effective from 1 September 1999

472 See Attorney-General's Department, *Legal Services Directions*, 1 September 1999, [2.1] and Appendix A.

473 See Ibid, [7.1], [7.2] and discussion at [8.151].

474 Ibid, Appendix B, 2.

475 'The duty also goes beyond the requirement for lawyers to act in accordance with their ethical obligations.' See Ibid, Appendix B, notes [3].

476 See Ibid, Appendix B, 2.

477 See Ibid, Appendix B, notes [4].

478 The Crown Prosecution Service (UK), *The Code for Crown Prosecutors*, <www.cps.gov.uk/home/CodeForCrownProsecutors/>, 6.5(i).

criminal matters.[479] The ALRC also asked whether the *Prosecution Policy of the Commonwealth*—which sets out the factors to be considered in making a prosecution decision—should be amended to specify the factors that will be relied upon by the DPP in making a decision whether to prosecute where there is a possibility that classified or security sensitive information will be revealed.[480]

8.284 One view is that it is difficult to see how the development of guidelines or the amendment of the *Prosecution Policy of the Commonwealth* could be done to any useful effect in light of the wide variety of circumstances that may arise. The result could be a source of frustration or difficulty for those making decisions on the Crown's behalf in these areas. In addition, guidelines and policies cannot be enforced.[481] No other submissions were received on this point. Accordingly, at this stage, the ALRC has not made a proposal in this regard, but remains interested in hearing any views on the issue.

8.285 In BP 8, the ALRC also asked whether guidelines should be developed for the disclosure, withholding or use of classified and sensitive information in civil cases.[482]

8.286 The NSW Law Society submitted that:

> It is not desirable for prescriptive guidelines to be issued concerning the disclosure, withholding or use of classified or sensitive information in civil matters, but consideration should be given to the development of appropriate directions from the Attorney-General as to the approach government parties and their representative should take in dealing with such issues in fulfilling their role as 'model litigants'.[483]

8.287 The ALRC is interested in hearing views about the need for the Attorney-General to develop directions to federal agencies about the approach they should take in acting in cases involving classified and security sensitive information—including but not limited to their duties to act as model litigants in such cases. The need for such directions may be more compelling in light of the proposals made in this Paper on a legislative scheme to deal with proceedings involving classified and security sensitive information—see Chapter 10.

---

479 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 64.

480 Ibid, Q 65. See also Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth*, <www.cdpp.gov.au/Prosecutions/Policy/>.

481 Advisory Committee member, *Correspondence*, 18 September 2003.

482 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 68.

483 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

Question 8–1 Should the Attorney-General issue Legal Services Directions pursuant to the *Judiciary Act 1903* (Cth) in relation to the approach that the Australian Government and its agencies should take in dealing with proceedings involving classified and security sensitive information, including any specific or additional duties which arise in fulfilling the duty to act as a model litigant?

9. Courts—Restricting a Party's Access

Contents

Introduction

9.1 Chapter 8 considered the use of methods in court and tribunal proceedings to restrict access to sensitive information to the public or to block the admission into evidence of such information. This chapter considers the more controversial use of methods in court and tribunal proceedings to restrict access to information to the party affected—namely the leading of, or reliance upon, secret evidence; and the conducting of secret hearings.

Secret evidence

9.2 One severe method of protecting classified or security sensitive information in investigations and proceedings is to deny parties and their lawyers access to any such material. In contrast to an in-camera hearing held in the presence of the defendant and his or her lawyer,[1] some hearings are closed to one or more parties or their lawyers. In effect, one party may seek to lead evidence in a court or tribunal closed to the party against whom the evidence is lead. However, there is a strong common law tradition against the use of secret evidence.

9.3 Apart from its inherent unfairness, the use of secret evidence 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

1 Except in the case of ex parte proceedings.

examine, or have examined, any adverse witnesses.[2] It also breaches the principle of equality of arms discussed in Chapter 7. 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 International Covenant on Civil and Political Rights (ICCPR) to communicate with, and be defended by, counsel of his or her own choosing.[3] 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.

9.4 Leading secret evidence in Australian courts in certain situations may also offend Chapter III of the *Australian Constitution.* This issue is discussed at [9.10] below.

9.5 In other cases, maintaining the secrecy of evidence led in court following a conviction could adversely affect the convicted person's ability to properly appeal their conviction. For example, Jonathan Pollard, a US naval intelligence analyst convicted of spying in 1987 has asked, and been refused, access to sealed government documents that the US Government alleges describe the impact of his spying.[4] Pollard's lawyers have expressed doubts about those claims and argue that the documents could assist them in influencing the President to commute Pollard's life sentence. In particular, his lawyers want to see a letter from former Defense Secretary Caspar Weinberger written to the court in 1987 that details the damage that Pollard's crime caused. Pollard's lawyers assert that the sealed documents may show that the US Government forecast damage from Pollard's spying that never eventuated, and that other spies may have committed some of the espionage for which Pollard has been found guilty. His lawyers claim that there is evidence that about 25 people, mostly employees of the US Department of Justice, have been granted access between 1993 and 2000 to the same material in respect of which Pollard's lawyers, who have security clearances, have been denied access.[5]

9.6 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.[6] 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

---

2 See ICCPR, Art 14(3), set out in Appendix 3. See also discussion on the use of secret evidence in *Van Mechelen v The Netherlands* (1997) III Eur Court HR 691 in Ch 7 at [7.39]–[7.41] and the discussion on secret evidence in non-criminal proceedings, including deportation proceedings in Ch 7 at [7.83]–[7.91].

3 Except for reasons such as the lawyer's conflict of interest or being a witness in his or her client's matter.

4 In November 2003, Chief US District Court Judge Thomas Hogan refused Pollard's request and dismissed his appeal to reduce his life sentence: C Leonnig, *Judge Rejects Spy's Life Sentence Appeal*, <www.washingtonpost.com/ac2/wp-dyn/A36213-2003Nov13?language=printer> at 13 November 2003.

5 C Leonnig, 'Pollard Seeks to Appeal Life Sentence', *The Washington Post*, 2 September 2003, <www.compuquick-consulting.com/jp/2003/090203e.htm>.

6 The INS was dissolved on 1 March 2003. Its enforcement and service functions were transferred to the 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), 14.

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.[7] In secret evidence proceedings, one party cannot cross-examine and often has no idea of the nature and extent of the evidence.[8]

9.7 Cole asserts that the INS's use of secret evidence contains practically no safeguards against abuse, stating 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 it.[9]

- Evidence has often been over-classified and there is no requirement that anyone review the classification decision.[10]

- The INS has failed to keep a record of many of its secret evidence presentations, thereby defeating meaningful review.[11]

- There is no requirement that the INS first attempt to make its case without relying on secret evidence.[12]

9.8 There is a real concern that secret proceedings tend to encourage reliance on questionable evidence, including double and triple hearsay. When the secret evidence consists of hearsay, it is impossible even for the judge to question the sources.[13] 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.[14] 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 or provide the context.

9.9 Cole has also been critical of the standard of declassified summaries of secret evidence provided by the INS to aliens, stating that these summaries 'are often so

---

7 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> at 23 May 2000, 2.

8 Ibid, 6.

9 Ibid, 2.

10 Ibid, 10.

11 Ibid, 2.

12 Ibid, 7.

13 Ibid, 11–12.

14 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> at 23 May 2000, 3.

general as to be entirely unhelpful'. He advocates the use of summaries that would give aliens 'a meaningful opportunity to respond'.[15] This raises the issue of whether there should be a legislative standard set for such summaries. The US *Classified Information Procedures Act*, s 6(c) (CIPA) requires that in criminal matters such a summary must provide the defendant 'with substantially the same ability to make his defense as would disclosure of the specified classified information'.

Courts closed to a party

Chapter III considerations in Australia

9.10 Australian courts exercising federal jurisdiction must exercise the judicial power of the Commonwealth in accordance with Chapter III of the *Australian Constitution*. Accordingly, special considerations apply in relation to the use of certain techniques to protect classified and security sensitive information in court hearings, as opposed to tribunal hearings, which are not subject to the provisions of Chapter III.[16] As indicated in the discussion below, legislation sanctioning reliance on secret evidence in a Chapter III court, especially where such evidence is central rather than incidental to a prosecution, runs the strong risk of being declared unconstitutional. However, not all forms of secret evidence run this risk. For example, a distinction can be made between secret evidence presented to a court to determine a claim for public interest immunity, where the successful outcome of that claim is that the material the subject of the claim is not ultimately adduced in evidence (and is therefore not relied upon by the court) and the adducing of secret evidence against a party upon which a court may rely. In the former case, confidential affidavits and confidential submissions of counsel supporting the claim are provided to the judge determining the claim:

> It is routine that such claims are dealt with in open court and are supported by some evidence which is open and is provided to the parties in the proceedings. The evidentiary basis of the claim is thus publicly exposed so far as can be done without revealing the nature or the content of the material for which the immunity is asserted.
>
> Under this procedure, the fact that the additional, confidential evidence has been provided to the Judge is not kept 'secret'. …
>
> This procedure works perfectly well.[17]

9.11 Another example of the use of secret evidence in Australian courts is the use of such evidence to determine whether the prosecution must disclose sensitive material to an accused person. For example, the *Justices Act 1902* (WA) specifies the material that the prosecution must serve on the accused prior to a committal mention.[18] The prosecution may apply to have any particular disclosure requirement dispensed with, without

---

15 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> at 23 May 2000.

16 However, legislation purporting to vest in administrative tribunals the judicial power or functions of a Chapter III court would be unconstitutional.

17 Advisory Committee member, *Correspondence*, 18 September 2003.

18 See *Justices Act 1902* (WA), s 103(1) and (2).

notice to the accused, and the application may be heard and determined in the absence of the accused.[19] The Act provides that:

> The room or place in which the justices hear and determine an application under subsection (4) is not to be regarded as an open court, and the justices may order that no person is to be in the room or place without their permission.[20]

9.12 The court may order that the prosecution does not have to comply with a particular pre-trial disclosure requirement if, on the application by the prosecution, the justices are satisfied that '(a) there is a good reason for doing so*;* and (b) no miscarriage of justice will result.'[21]

9.13 Section 71 of the *Australian Constitution*[22] establishes the High Court as the principal repository of the judicial power of the Commonwealth, and provides that Parliament may vest federal judicial power in other federal courts that it creates, and in such other courts as it invests with federal jurisdiction.[23] The Australian Parliament may not invest federal courts or any state Supreme Court capable of exercising federal jurisdiction with functions that are incompatible with the proper exercise of judicial power under Chapter III. Similarly, a state legislature may not invest that State's Supreme Court with a function that is incompatible with the exercise by that Court of the judicial power of the Commonwealth.[24]

9.14 The *Australian Constitution* contains no express right to a fair trial. However, in recent years there have been some judicial references to the potential implied protection of various rights or guarantees under Chapter III, the most prominent examples being the right to a fair trial and the right to due process. As discussed in Chapter 7,[25] Gaudron and Deane JJ in *Dietrich v R* held that the right to a fair trial was entrenched in Chapter III of the *Australian Constitution*.[26] Gaudron J also expressed the view in *Re Nolan; ex parte Young* that:

> Because it is an essential feature of judicial power that it be exercised in accordance with the judicial process, Ch III provides a guarantee, albeit only by implication, of a fair trial of those offences created by a law of the Commonwealth which must be tried in the courts named or indicated in s 71. Conversely, there is no such guarantee with

---

19 See Ibid, s 103(4) and (5).
20 Ibid, s 103(6).
21 Ibid, s 4. The ALRC's views on this scheme are set out in Ch 10.
22 Set out in Appendix 3.
23 See Australian Law Reform Commission, *The Judicial Power of the Commonwealth*, ALRC 92 (2001).
24 See *Kable v Director of Public Prosecutions (NSW)* (1996) 189 CLR 51.
25 See Ch 7 at [7.42]–[7.43].
26 Mason CJ, Toohey and McHugh JJ, who comprised the other members of the majority in *Dietrich v The Queen* (1992) 177 CLR 292, were silent as to the constitutional issue, although they agreed that the right to a fair trial existed at common law. See F Wheeler, 'The Doctrine of Separation of Powers and Constitutionally Entrenched Due Process in Australia' (1997) 23 *Monash University Law Review* 248, fn 116; J Hope, 'A Constitutional Right to a Fair Trial? Implications for the Reform of the Australian Criminal Justice System' (1996) 24 *Federal Law Review* 173. Brennan and Dawson JJ dissented in *Dietrich v The Queen* (1992) 177 CLR 292. Kirby J in *Cameron v The Queen* [2002] HCA 6, [97] stated that *Dietrich* rested on a 'broader, and possibly constitutional foundation' such as 'the implied constitutional right to due process of law'.

> respect to offences, if any, which may be tried in the exercise of non-judicial power by some other body or tribunal.[27]

9.15 As noted by one commentator,[28] Justice Kirby has also kept alive the notion of an implied right to a fair trial in recent dicta.[29]

9.16 However, '[t]o date, no human right or individual guarantee has been implied by a majority of the High Court from Chapter III of the [*Australian Constitution*].'[30] It remains to be seen whether a majority of the High Court will imply from Chapter III a constitutional guarantee to a fair trial. One commentator has remarked that, of all the due process principles, 'the notion that there is an implied guarantee of a fair trial of a federal offence has the greatest prospect of future development.'[31] However, 'even if a majority of the High Court were to adopt the view that the [*Australian Constitution*] contains an implied right to a fair trial, a great many answers about the content, scope and nature of that right would still need to be answered.'[32]

9.17 The view has been expressed that confusion has been introduced by constitutionalising the issue rather than leaving it to the common law:

> [T]here are real drawbacks to the characterisation of the right to a fair trial as a constitutional rather than a common law right. From the point of view of governments searching for the proper balance between protecting the interests of the individual accused and ensuring that the system itself does not collapse under the weight of complicated procedural rules, the threat of having legislation declared invalid on unpredictable grounds can only act as a general deterrent to introducing any changes at all, bad or good. …
>
> In summary, for both governments and the courts, the constitutionalism of the right to a fair trial could mean the worst of both worlds: uncertainty, without flexibility.[33]

---

27 *Re Nolan; Ex parte Young* (1991) 172 CLR 460, 496.

28 See F Wheeler, 'Due Process, Judicial Power and Chapter III: An Evolving Guarantee' (Paper presented at The Australian Constitution in Troubled Times conference, Canberra, 7–9 November 2003), 54.

29 For example, in *Crampton v The Queen* [2000] HCA 60, [127] Kirby J stated 'It will usually be proper for the trial judge to bring appropriate considerations to the specific notice of the jury by way of comment. Such considerations do not, however, relieve the trial judge of the paramount duty imposed by the law (and quite possibly implied in the Constitution) to ensure the fair trial of a person accused of a serious criminal offence.' See also *Bull v The Queen; King v The Queen; Marotta v The Queen* [2000] HCA 24, [137] (Kirby J); *Ng v The Queen* [2003] HCA 20, [77] (Kirby J); and *Roberts v Bass* [2002] HCA 57, [145] (Kirby J).

30 W Lacey, 'Inherent Jurisdiction, Judicial Power and Implied Guarantees under Chapter III of the Constitution' (2003) 31(1) *Federal Law Review* 57, 71.

31 F Wheeler, 'Due Process, Judicial Power and Chapter III: An Evolving Guarantee' (Paper presented at The Australian Constitution in Troubled Times conference, Canberra, 7–9 November 2003), 53.

32 J Hope, 'A Constitutional Right to a Fair Trial? Implications for the Reform of the Australian Criminal Justice System' (1996) 24 *Federal Law Review* 173, 196.

33 Ibid, 198. For example, Hope states that a consequence of the recognition of a constitutionally entrenched right to a fair trial would be that the validity of certain legislation affecting the rights of an accused person would become vulnerable to challenge. Such legislation includes that which places the persuasive or evidentiary burden of proof on an accused, introduces new offences of strict liability, or prohibits certain grounds of defence in relation to some offences. See J Hope, 'A Constitutional Right to a Fair Trial?

9.18 One commentator argues that what is actually protected by Chapter III is not specific guarantees for individuals but rather the inherent power of federal courts to protect the judicial process in the administration of justice, the effect of which may be to protect various procedural rights, such as the court's power to stay proceedings, where justice demands it.[34] Other commentators are of the view that a guarantee of due process can and should be implied from the operation of Chapter III rather than the inherent powers of the court.[35] Justice McHugh has stated that it 'is only in recent years that it has become accepted that due process rights are guaranteed by the Constitution'.[36] An example of such a due process right recognised as protected by Chapter III is the right to legal representation in certain situations.[37]

9.19 High Court judges have often observed that 'judicial power' for the purposes of Chapter III has never been exhaustively defined but a number of statements have been made identifying its essential components. In *Huddart, Parker & Co Pty Ltd v Moorehead*, Griffith CJ stated that:

> [T]he words 'judicial power' as used in s 71 of the Constitution mean the power which every sovereign authority must of necessity have to decide controversies between its subjects, or between itself and its subjects, whether the rights relate to life, liberty or property. The exercise of this power does not begin until some tribunal which has power to give a binding and authoritative decision (whether subject to appeal or not) is called upon to take action.[38]

9.20 In *Nicholas v The Queen*,[39] Gaudron J stated:

> The difficulties involved in defining 'judicial power' are well known. In general terms, however, it is that power which is brought to bear in making binding determinations as to guilt or innocence, in making binding determinations as to rights, liabilities, powers, duties or status put in issue in justiciable controversies, and in making adjustment of rights and interests in accordance with legal standards. It is a power which is exercised in accordance with the judicial process and in that process, many specific and ancillary powers are also exercised. One ancillary power which may be exercised in that process is the power to exclude evidence in the exercise of a discretion which permits that course. …
>
> Judicial power is not adequately defined solely in terms of the nature and subject-matter of determinations made in exercise of that power. It must also be defined in terms that recognise it is a power exercised by courts and exercised by them in accor-

---

Implications for the Reform of the Australian Criminal Justice System' (1996) 24 *Federal Law Review* 173, 189–191.

34 See W Lacey, 'Inherent Jurisdiction, Judicial Power and Implied Guarantees under Chapter III of the Constitution' (2003) 31(1) *Federal Law Review* 57, 59–60 and 71.

35 See F Wheeler, 'The Doctrine of Separation of Powers and Constitutionally Entrenched Due Process in Australia' (1997) 23 *Monash University Law Review* 248, 254.

36 Justice M McHugh, 'Does Chapter III of the Constitution Protect Substantive as well as Procedural Rights?' (2001) 21 *Australian Bar Review* 235, 238.

37 See Ibid, 240 and see *Dietrich v The Queen* (1992) 177 CLR 292.

38 *Huddart, Parker & Co Pty Ltd v Moorehead* (1909) 8 CLR 330, 357.

39 In this case, a majority of the High Court upheld the constitutional validity of the *Crimes Amendment (Controlled Operations) Act 1996* (NSW). The Act was held not to be an impermissible interference with the exercise of judicial power.

> dance with the judicial process. Thus, as was said in *Chu Kheng Lim v Minister for Immigration*, the Parliament cannot make 'a law which requires or authorises the courts in which the judicial power of the Commonwealth is exclusively vested to exercise judicial power in a manner that is inconsistent with the essential character of a court or with the nature of judicial power.'[40]
>
> In my view, consistency with the essential character of a court and with the nature of judicial power necessitates that a court not be required or authorised to proceed in a manner that does not ensure equality before the law, impartiality and the appearance of impartiality,[41] the right of a party to meet the case against him or her, the independent determination of the matter in controversy by application of the law to the facts determined in accordance with rules and procedures which truly permit the facts to be ascertained and, in the case of criminal proceedings, the determination of guilt or innocence by means of fair trial according to law. It means, moreover, that a court cannot be required or authorised to proceed in any manner which involves an abuse of process, which would render its proceedings inefficacious, or which tends to bring the administration of justice into disrepute.[42]

9.21 In *Bass v Permanent Trustee Co Ltd*, the High Court recognised that judicial power involved the 'application of the relevant law to facts as found in proceedings conducted in accordance with the judicial process' and that this required that the 'parties be given an opportunity to present their evidence and to challenge the evidence led against them'.[43]

9.22 A further element of judicial power that has been identified in cases is the need to act in accordance with the principles of natural justice.[44]

9.23 The judicial process also embraces the requirement that courts proceed, except in exceptional circumstances, by way of open and public hearings. Justice Gaudron

---

40 *Chu Kheng Lim v Minister for Immigration* (1992) 176 CLR 1, 27 (Brennan, Deane and Dawson JJ).

41 Brennan CJ also expressed the view that a court exercising judicial power must act, and be seen to be acting, impartially: *Nicholas v The Queen* [1998] HCA 9, [20]. Gaudron J stated in *Ebner v Official Trustee in Bankruptcy* [2000] HCA 63 at [79]–[82] that '[i]mpartiality and the appearance of impartiality are so fundamental to the judicial process that they are defining features of judicial power' and that Chapter III 'operates to guarantee impartiality and the appearance of impartiality throughout the Australian court system'. Kirby J in *Ebner v Official Trustee in Bankruptcy* [2000] HCA 63, [116] expressed the view that 'in Australia, the ultimate foundation for the judicial requirements of independence and impartiality rests on the requirements of, and implications derived from, Chapter III of the Constitution' (citations omitted).

42 *Nicholas v The Queen* [1998] HCA 9, [70], [73] and [74] (citations omitted).

43 *Bass v Permanent Trustee Co Ltd* (1999) 198 CLR 334, 359 (Gleeson CJ, Gaudron, McHugh, Gummow, Hayne and Callinan JJ).

44 See *Harris v Caladine* (1991) 172 CLR 84, 150, where Gaudron J stated that the judicial power 'involves the application of the rules of natural justice'; *Leeth v The Commonwealth* (1992) 174 CLR 455, 470 (Mason CJ, Dawson and McHugh JJ): 'it may well be that any attempt on the part of the legislature to cause a court to act in a manner contrary to natural justice would impose a non-judicial requirement inconsistent with the exercise of judicial power' and *Re Refugee Review Tribunal; Ex parte Aala* [2000] HCA 57, [41] (Gaudron and Gummow JJ) 'procedural fairness is a concomitant of the vesting of the judicial power of the Commonwealth in [a] federal court'. See also F Wheeler, 'The Doctrine of Separation of Powers and Constitutionally Entrenched Due Process in Australia' (1997) 23 *Monash University Law Review* 248, 252 on this point.

made the following observations in *Re Nolan; Ex Parte Young* in relation to judicial process:

> The determination in accordance with the judicial process of controversies as to legal rights and obligations and as to the legal consequences attaching to conduct is vital to the maintenance of an open, just and free society. Quite apart from the public's right to know what matters are being determined in the courts and with what consequences, open and public proceedings are necessary in the public interest because secrecy is conducive to the abuse of power and, thus, to injustice. Moreover and more directly, the judicial process protects the individual from arbitrary punishment and the arbitrary abrogation of rights by ensuring that punishment is not inflicted and rights are not interfered with other than in consequence of the fair and impartial application of the relevant law to facts which have been properly ascertained.[45]

9.24 A number of the elements of judicial power identified above suggest that it could be unconstitutional to require or authorise a Chapter III court to receive and rely on secret evidence in court proceedings, particularly criminal proceedings where the secret evidence is central to the indictment. These elements include authorising a court to proceed in a manner that does not ensure impartiality, or 'the right of a party to meet the case against him or her' or does not allow for 'the determination of facts in accordance with rules and procedures which truly permit the facts to be ascertained' or does not adhere to the principles of natural justice. Where evidence is led against a party in his or her absence, without that party knowing the substance of that evidence and without having the opportunity to test that evidence through the process of cross-examination, the court's ability to act impartially is impeded,[46] a party's 'right to meet the case against him or her' and to be heard in accordance with natural justice principles is diminished, and it is questionable that the process is conducive to 'truly permit[ting] the facts to be ascertained'. Further, such a process could arguably involve an abuse of process and adversely impact on the right to a fair trial.

9.25 However, it may be argued that Chapter III should not be interpreted so as to defeat itself. The administration of justice calls for an ability to prosecute serious national security cases, and there are cases where access by the accused to evidence would defeat the administration of justice by reasonably leading to a prosecutorial decision to abort the prosecution.[47] Such an argument is persuasive where classified or security sensitive evidence is peripheral to a prosecution. There is a greater risk that denying an accused access to classified or security sensitive evidence which is central to the indictment would be found to be contrary to natural justice.

---

45 *Re Nolan; Ex parte Young* (1991) 172 CLR 460, 496–497. See also *Harris v Caladine* (1991) 172 CLR 84, 150 (Gaudron J) and *Grollo v Palmer* (1995) 184 CLR 348, 379, where McHugh J stated: 'Open justice is the hallmark of the common law system of justice and is an essential characteristic of the exercise of federal judicial power'. See also the discussion on open justice in Ch 7.

46 See comments on a court's ability to act impartially in *Re Criminal Proceeds Confiscation Act 2002 (Qld)* [2003] QCA 249, discussed at [9.26]–[9.28] below.

47 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003.

9.26 In *Re Criminal Proceeds Confiscation Act 2002 (Qld)*, the Queensland Court of Appeal declared s 30 of the *Criminal Proceeds Confiscation Act 2002* (Qld) to be constitutionally invalid as its interference with the essential character of the exercise of judicial power was repugnant to, or incompatible with, the exercise of the judicial power of the Commonwealth. Section 30 directed the court to hear and determine an application for an order restraining property from being dealt with in the absence of any interested party, including both the person alleged to have engaged in illegal activity and the innocent property owner. Section 30(3) provided:

> [T]he court must hear the application—
>
> (a) in the absence of a person whose property is the subject of the application; and
>
> (b) without the relevant person having being informed of the application.

9.27 Williams J, with whom White and Wilson JJ agreed, stated that the provision amounted to a 'legislative command' to a judge to proceed in that manner.[48] The Court distinguished the operation of the provision from the hearing of an ex parte application, where the court maintains the discretion whether to proceed ex parte:

> In appropriate cases the judge would decline to hear the matter ex parte, the order made would be on an interim basis only, would provide for service of all material on the party affected, and would ensure that the party affected was not adversely affected by the making of the interim order. … The ex parte hearing and the subsequent hearing on notice would comply with the requirements of proper judicial process. Because the judge was in control of the proceedings at all times there would be no infringement of the rights of natural justice and there would be no impairment of the judicial process.[49]

9.28 Williams J noted that the Supreme Court had to be satisfied that the public interest did not require the court to refuse to make the order:

> How could a judge possibly be so satisfied in the exercise of judicial power when the only entity entitled to place material before the court on which a judgment on that issue could be formed was the State? Similarly, how could a judge possibly determine whether or not it was appropriate to require the State to give an undertaking as to damages and costs when the only entity entitled to place material before the court was the State? Asking a judge to make a decision on such issues in those circumstances makes a mockery of the exercise of the judicial power in question. The statutory provision removes the essential protection of the citizen inherent in the judicial process. Effectively the provision directs the court to hear the matter in a manner which ensures that the outcome will be adverse to the citizen and deprives the court of the capacity to act impartially.[50]

---

48 *Re Criminal Proceeds Confiscation Act 2002 (Qld)* [2003] QCA 249, [11].
49 Ibid, [31].
50 Ibid, [57].

9.29 The validity of the *Crimes* (*Confiscation of Profits) Act 1988* (WA) (now repealed) was considered by the WA Court of Appeal[51] and is now the subject of a special leave application before the High Court.[52] The issue before the Court of Appeal was whether certain sections of the Act, which deemed a deceased person to have been convicted of serious offences for the purposes of the Act, thereby making his or her estate liable to confiscation orders under the Act, were invalid and inoperative. The effect of s 3 of the Act in the case under consideration was that the person who had died before trial had been taken to have absconded and was deemed to have been convicted of a serious offence for the purposes of the Act, even though he had never had a trial and had pleaded not guilty. Wallwork J, in the minority, held that the provisions of the Act 'were invalid and inoperative because they were inconsistent with the proper exercise of the judicial power of the Supreme Court of Western Australia.'[53]

9.30 Wallwork J stated that the Act:

> did in effect deprive the deceased of the right to meet the case against him and it did not permit the independent determination of the matter in controversy by the application of the law to the facts determined in accordance with rules and procedures.[54]

9.31 On appeal, the majority in *Silbert v Director of Public Prosecutions for Western Australia* upheld the validity of the legislation. The majority emphasised that the Court could only make a forfeiture or pecuniary penalty order against the estate of the deceased if it was satisfied beyond reasonable doubt that the person committed the offence and that the penalty to be forfeited was used in, or in connection with, the commission of the offence or was derived or realised as a result of the commission of the offence.[55] The Act did not give a direction to the Supreme Court to find anyone guilty.[56]

9.32 Denying the court any ultimate discretion was a key factor in rendering invalid the legislation under consideration in *Re Criminal Proceeds Confiscation Act 2002 (Qld)*, and that factor was also at play in rendering invalid the legislation before the High Court in *Kable v The Director of Public Prosecutions*.[57] Importantly, In *Nicholas v The Queen*, Brennan J stated that:

---

51 See *Silbert v Director of Public Prosecutions for Western Australia* [2002] WASCA 12.

52 See *Silbert v Director of Public Prosecutions for Western Australia*, High Court of Australia Case no P16 of 2002, Transcript of proceedings on 9 May 2003, where Kirby and McHugh JJ ordered that the application for special leave be referred to the Full Bench of the High Court and that it be argued as if it were an appeal.

53 *Silbert v Director of Public Prosecutions for Western Australia* [2002] WASCA 12, [53].

54 Ibid, [19].

55 Ibid, [79], [82].

56 Ibid, [78].

57 See *Kable v Director of Public Prosecutions (NSW)* (1996) 189 CLR 51, 123 (McHugh J). See also *Amended A-G (Qld) v Fardon* [2003] QCA 416, [21], which, in upholding the constitutionality of the *Dangerous Prisoners (Sexual Offenders) Act 2003* (Qld), distinguished the legislative scheme from the one considered in *Kable v Director of Public Prosecutions (NSW)* (1996) 189 CLR 51 on various bases, including that the Queensland legislation conferred the court with a genuine discretionary power, and that the criterion informing the exercise of that discretion was community protection rather than punishment.

> A law that purports to direct the manner in which judicial power should be exercised is constitutionally invalid. However, a law which merely prescribes a court's practice or procedure does not direct the exercise of the judicial power in finding facts, applying law or exercising an available discretion.[58]

9.33 In light of the above, it appears that legislation which gives a court discretion (as opposed to a direction) to receive secret evidence in particular circumstances may not offend Chapter III of the *Australian Constitution.* However, there is still a risk that the grant of that discretion will amount to an authorisation (as opposed to a requirement) for a Chapter III court to exercise judicial power in a manner that is inconsistent with the essential character of a court or with the nature of judicial power. As noted above,[59] the High Court in *Chu Kheng Lim v Minister for Immigration*,[60] and Gaudron J in *Nicholas v The Queen*[61] stated that Parliament could neither require nor *authorise* a law which allowed the courts to act in such a manner.

Overseas

9.34 The *Terrorism Act 2000* (UK) provides for a number of counter-terrorist police powers. A constable may arrest without a warrant a person whom he or she reasonably suspects to be a terrorist.[62] The maximum period of detention is 48 hours, but this can be extended if a police officer applies to a judicial authority for the issue of a warrant for further detention.[63] The Act provides that the person to whom an application for further detention relates shall be entitled to make representations to the judicial authority about the application and, subject to certain exceptions, shall be entitled to be legally represented at the hearing.[64] The exceptions are that the judicial authority has the discretion to exclude from any part of the hearing the person to whom the application relates and anyone representing that person.[65] In addition, the police officer who made the application may apply to the judicial authority for an order that specified information on which he or she intends to rely be withheld from the person to whom the application relates and anyone representing him or her.[66] The judicial authority must then make an order excluding the person to whom the application relates and anyone representing him or her from the hearing of the application in relation to the withholding of information.[67] The Act sets out the circumstances in which the judicial authority may make an order to withhold information, including where there are reasonable grounds for believing that, if the information were disclosed:

---

58 *Nicholas v The Queen* [1998] HCA 9, [20].
59 At [9.20].
60 *Chu Kheng Lim v Minister for Immigration* (1992) 176 CLR 1, 27 (Brennan, Deane and Dawson JJ). This view was also cited with approval by Gummow J in *Nicholas v The Queen* [1998] HCA 9, [146]; and Brennan CJ in *Nicholas v The Queen* [1998] HCA 9, [13].
61 *Nicholas v The Queen* [1998] HCA 9, [74].
62 *Terrorism Act 2000* (UK), s 41.
63 Ibid, Sch 8, Part III.
64 Ibid, Sch 8, [33(1)].
65 Ibid, Sch 8, [33(3)].
66 Ibid, Sch 8, [34(1)].
67 Ibid, Sch 8, [34(4)].

> (e) the prevention of an act of terrorism would be made more difficult as a result of a person being alerted;
>
> (f) the gathering of information about the commission, preparation or instigation of an act of terrorism would be interfered with; … [68]

9.35 The Canadian *Criminal Code*[69] provides for certain hearings to be conducted in the absence of a party and its legal representative, and for evidence led in a such a proceeding to be relied upon by a judge. Provision is made for the Governor in Council, on the recommendation of the Solicitor General, to place an entity on an established list of terrorist organisations.[70] An organisation may make an application in writing to the Solicitor General to decide whether there are reasonable grounds to recommend to the Governor in Council that the applicant no longer be a listed entity.[71] The Code provides for the applicant to apply to a judge for judicial review of a decision made in respect of its application.[72] In reviewing the decision, the judge must:

> (a) examine, in private, any security or criminal intelligence reports considered in listing the applicant and hear any other evidence or information that may be presented by or on behalf of the Solicitor General and may, at the request of the Solicitor General, hear all or part of the evidence or information in the absence of the applicant and any counsel representing the applicant, if the judge is of the opinion that the disclosure of the information would injure national security or endanger the safety of any person;
>
> (b) provide the applicant with a statement summarizing the information available to the judge so as to enable the applicant to be reasonably informed of the reasons for the decision, without disclosing any information the disclosure of which would, in the judge's opinion, injure national security or endanger the safety of any person;
>
> (c) provide the applicant with a reasonable opportunity to be heard; and
>
> (d) determine whether the decision is reasonable on the basis of the information available to the judge and, if found not to be reasonable, order that the applicant no longer be a listed entity.[73]

9.36 The Code further provides that, for the purposes of the review, in private and in the absence of the applicant or any counsel representing it:

> (a) the Solicitor General of Canada may make an application to the judge for the admission of information obtained in confidence from a government, an institution or an agency of a foreign state, from an international organization of states or from an institution or an agency of an international organization of states; and

---

68 Ibid, Sch 8, [34(2)].
69 [RS 1985, c C-46].
70 *Criminal Code* [RS 1985, c C–46] (Canada), s 83.05(1).
71 Ibid, s 83.05(2).
72 Ibid, s 83.05(3).
73 Ibid, s 83.05(6).

> (b) the judge shall examine the information and provide counsel representing the Solicitor General with a reasonable opportunity to be heard as to whether the information is relevant but should not be disclosed to the applicant or any counsel representing it because the disclosure would injure national security or endanger the safety of any person.[74]

9.37 If the judge determines that the information is relevant but that its disclosure would harm national security or endanger the safety of any person, the information is not to be provided to the applicant in the summary of the information available to the court—but the court is nevertheless empowered to base its determination of the review of the application on it.[75] The Code specifies the circumstances in which the judge is precluded from relying on the information in making his or her determination, which include where the judge determines that the information is not relevant.[76]

9.38 The *Charities Registration (Security Information) Act 2001* (Canada) has as one of its purposes 'to demonstrate Canada's commitment to participating in concerted international efforts to deny support to those who engage in terrorist activities'.[77] The Act provides for the Solicitor General and the Minister of Revenue to sign a certificate stating, among other things, that in their opinion based on information[78] there are reasonable grounds to believe that an applicant[79] or registered charity made available resources to a defined entity that was, and continues to be, engaged in terrorist activities as defined.[80] A judge must determine whether the certificate is reasonable on the basis of the information and evidence available.[81] Judicial consideration of the certificate is governed by the following provisions, which include excluding the applicant or registered charity from the hearing of evidence:

> (b) the judge shall ensure the confidentiality of the information on which the certificate is based and of any other evidence that may be provided to the judge if, in the opinion of the judge, its disclosure would be injurious to national security or endanger the safety of any person; …
>
> (d) the judge, shall, without delay after the matter is referred to the Federal Court, examine the information and any other evidence in private;
>
> (e) on each request of the Minister or the Minister of National Revenue, the judge shall hear all or part of the evidence in the absence of the applicant or registered charity named in the certificate and their counsel if, in the opinion of the judge, its disclosure would be injurious to national security or endanger the safety of any person; …

---

74 Ibid, s 83.06(1).
75 Ibid, s 83.06(3).
76 Ibid, s 83.06(2)(b).
77 *Charities Registration (Security Information) Act 2001* (Canada), s 2(1).
78 'Information' is defined as 'security or criminal intelligence information and information that is obtained in confidence from a source in Canada, from the government of a foreign state, from an international organization of states or from an institution of such a government or organization': Ibid, s 3.
79 'Applicant' is defined as 'a corporation, an organization or a trust that applies to the Minister of National Revenue to become a registered charity: Ibid, s 3.
80 See Ibid, s 4.
81 Ibid, s 7(1).

> (h) the judge shall provide the applicant or registered charity with a summary of the information or evidence that enables it to be reasonably informed of the circumstances giving rise to the certificate, but that does not include anything that in the opinion of the judge would be injurious to national security or endanger the safety of any person if disclosed;
>
> (i) the judge shall provide the applicant or registered charity with an opportunity to be heard; … [82]

Tribunals closed to a party

Australia

9.39 There are provisions allowing for secret evidence in various Australian tribunals including the Administrative Appeals Tribunal (AAT), the Refugee Review Tribunal (RRT), the Migration Review Tribunal (MRT) and the NSW Administrative Decisions Tribunal. Provisions allowing the use of secret evidence in the RRT and MRT are discussed below.[83]

9.40 The *Administrative Appeals Tribunal Act 1975* (Cth) (the AAT Act) provides that, where it is satisfied that it is desirable to do so by reason of the confidential nature of any evidence or matter or for any other reason, the AAT may prohibit or restrict the disclosure to some or all of the parties to a proceeding of evidence given before the AAT, or of the contents of a document lodged with, or received in evidence by, the AAT in relation to a proceeding.[84] In considering whether disclosure to some or all of the parties should be prohibited or restricted, the AAT:

> shall take as the basis of its consideration the principle that it is desirable that hearings of proceedings before [it] should be held in public and that evidence given before [it] and the contents of documents lodged with [it] or received in evidence by [it] should be made available to the public and to all the parties, but shall pay due regard to any reasons given to [it] why the hearing should be held in private or why publication or disclosure of the evidence or the matter contained in the document should be prohibited or restricted.[85]

9.41 Where the Attorney-General has certified that disclosure to a person of the whole or part of the statement of grounds contained in a qualified or adverse security assessment in respect of the person would be prejudicial to the interests of security[86] and an application is made to the AAT for a review of the security assessment, the Director-General of Security must lodge with the AAT a copy of the certificate and of the whole security assessment.[87] The AAT is prohibited from telling the applicant of

---

82 Ibid, s 6.
83 Under the heading 'Immigration cases' at [9.53].
84 *Administrative Appeals Tribunal Act 1975* (Cth), s 35(2)(c). See also *Administrative Decisions Tribunal Act 1997* (NSW), s 75(2).
85 *Administrative Appeals Tribunal Act 1975* (Cth), s 35(3)(b).
86 *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(b) allows the Attorney-General to make such a certification and to deliver it to the Director-General of Security.
87 *Administrative Appeals Tribunal Act 1975* (Cth), s 38A(1).

the existence of the certificate or from giving the applicant access to a copy of the certificate, or particulars of it or of any matter to which the certificate relates.[88]

9.42 The provision in the AAT Act governing the procedure of hearings concerning the review of security assessments before the Security Appeals Division allows secret evidence to be led. Applications for review of a security assessment in the Security Appeals Division of the AAT are to be heard in private and the AAT may determine who may be present at a hearing at any time.[89] 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 given, the applicant may not be present when the evidence is adduced or the submissions made; nor can the person's legal representative be present, unless the Minister consents.[90] If the representative is permitted to be present, he or she is prevented from disclosing to the applicant any such evidence or submissions.[91] It has been reported that such certificates are issued quite often.[92]

9.43 Michael Sassella, Senior Member of the AAT, has stated:

> [T]he procedures laid down in s 39A of the AAT Act contemplate that an applicant in a security appeal will not necessarily know all the details of the case against him or her. This is in contrast to s 39 of the AAT Act which requires the Tribunal to ensure, with minor exceptions, that every party to a proceeding is given a reasonable opportunity to present his or her case and to inspect any documents to which the Tribunal proposes to have regard in reaching a decision. Section 39 contemplates all parties being able to make submissions on those documents.
>
> Thus, it could be said that the justice available to security [assessment] appeals applicants is decidedly inferior to that generally available. This is broadly correct. However, it is also arguably justifiable, as a matter of policy given the context behind these appeals. ...
>
> The legislation affecting the Tribunal's procedures in these appeals appears calculated to bring about a result that is less than ideal from a natural justice perspective. However, it is possibly the case that the Tribunal's scrutiny in the security cases brought before it has been one of the influences encouraging a substantial fairness on ASIO's part in conducting security assessments.[93]

---

88 Ibid, s 38A(2).
89 Ibid, s 39A(5).
90 Ibid, s 39A(9).
91 Ibid, s 39A(10).
92 See 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. The author does, however, state that the applicant can generally be present when ASIO or the Commonwealth agency is presenting submissions: see fn 16 in that paper.
93 Ibid, 9–10.

9.44 The President of the AAT has expressed concern about:

> the problems which arise when parties and legal advisers are required to be excluded from a hearing and never see the evidence before the Tribunal. This is not a matter over which the Tribunal has any real control where the Attorney-General gives appropriate certificates under the Act. Having heard cases in the Security Appeals Division of the Tribunal, I am also aware of the fact that it can be necessary for material to be withheld from applicants before the Tribunal. … it can be difficult to balance the interests of an applicant who has a right to have a decision reviewed and a prima facie right to know what was the basis for the decision with the requirements of protecting national security. …
>
> It is certainly true to say that there are a greater number of matters in the Security Appeals Division of the Tribunal which raise these issues than there have been in the past. In previous years the matters in the Security Appeals [Division] of the Tribunal have largely been confined to appeals from adverse security assessments of Commonwealth public servants. The Minister for Foreign Affairs and Trade has recently cancelled a number of passports as a result of adverse security assessments and these have given rise to appeals in the Tribunal in which issues much wider than the security assessments of Commonwealth Public Servants are raised.[94]

9.45 As this submission shows, the use of secret evidence in the AAT has repercussions in immigration matters, such as cases involving passport cancellations.[95]

9.46 The AAT Act provides that, for the purposes of the Act, 'the question of whether information, or matter contained in a document, should be disclosed to the parties to a proceeding' is a question of law.[96] The effect of this is that a party to a proceeding before the AAT may appeal the decision to the Federal Court of Australia.[97]

Overseas

9.47 Some UK tribunals and commissions allow for the use of secret evidence. 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.[98] 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.[99] A person aggrieved by such directions may appeal to

---

94 Administrative Appeals Tribunal, *Submission CSSI 3*, 28 May 2003.

95 Secret evidence in immigration matters is discussed at [9.53] below.

96 *Administrative Appeals Tribunal Act 1975* (Cth), s 36D(2)(a). The section does not apply to proceedings before the Security Appeals Division to which s 39A applies, ie proceedings involving applications for review of security assessments.

97 See Ibid, s 44(1).

98 *Explanatory Notes to Anti-Terrorism, Crime and Security Act 2001* (UK), point 3.

99 *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.'

the Pathogens Access Appeals Commission.[100] 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) …[101]

9.48 The *Terrorism Act 2000* (UK) allows for rules to be made excluding an applicant and his or her legal representative from proceedings before the Proscribed Organisations Appeal Commission (POAC). The Act provides for the Secretary of State to proscribe, by order, an organisation if it is concerned in terrorism.[102] An appeal against proscription may be made to the POAC.[103] The Lord Chancellor may make rules prescribing the practice and procedure to be adhered to in proceedings before the POAC, having regard to the need to ensure that information is not disclosed contrary to the public interest.[104] In particular, the rules may:

> (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) …[105]

9.49 Until January 2003 the Investigatory Powers Tribunal was required to hold all hearings in private.[106] In addition, the *Regulation of Investigatory Powers Act 2000* (UK) enables the Secretary of State to make rules:

> (a) enabling or requiring the Tribunal to hear or consider any proceedings, complaint or reference without the person who brought the proceedings or made the complaint or reference having been given full particulars of the reasons for any conduct which is the subject of the proceedings, complaint or reference;

---

100 Ibid, s 70.

101 Ibid, Sch 6, s 5(3). Schedule 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'.

102 *Terrorism Act 2000* (UK), s 3. Section 3(5) provides that an organisation is concerned in terrorism if it 'commits or participates in acts of terrorism', 'prepares for terrorism', 'promotes or encourages terrorism' or 'is otherwise concerned in terrorism.'

103 Ibid, s 5.

104 Ibid, Sch 3, 5(1)(b) and 5(2)(b).

105 Ibid, Sch 3, 4(b) and (c). Liberty, a civil liberties organisation, has expressed concerns in relation to the de-proscription proceedings before POAC; in particular, whether the procedures infringe the right to a fair and impartial hearing enshrined in Art 6 of the European Convention of Human Rights. 'If one's claim was heard through regular judicial review proceedings, a number of safeguards could be relied upon: it is public, there are certain rules regulating the admissibility of evidence, burden of proof, and so on. In a POAC proceeding, the Lord Chancellor can design all procedural rules: he may decide to suspend the universally recognised safeguards which apply (including those relating to the admissibility of evidence and onus of proof) in all democratic conceptions of fair and impartial hearings': see Liberty, *Anti-Terrorism Legislation in the United Kingdom* (2002), 9.

106 See *In the Investigatory Powers Tribunal In Camera—In the Matter of Applications Nos IPT/01/62 and IPT/01/77—Draft Rulings of the Commission on Preliminary Issues of Law*, 23 January 2003.

> (b) enabling or requiring the Tribunal to take any steps in exercise of their jurisdiction in the absence of any person (including the person bringing the proceedings or making the complaint or reference and any legal representative of his);
>
> (c) enabling or requiring the Tribunal to give a summary of any evidence taken in his absence to the person by whom the proceedings were brought, or as the case may be, to the person who made the complaint or reference … [107]

9.50 The Investigatory Powers Tribunal Rules 2000 provide that the Tribunal is not to disclose to a complainant or any other person the fact that the Tribunal has held, or proposes to hold, an oral hearing under rule 9(4),[108] although it may make such a disclosure if the person required to attend the hearing has consented.[109] The Tribunal is also prohibited from disclosing to the complainant or any other person any information or document disclosed or provided to the Tribunal in the course of that hearing, or the identity of any witness at the hearing, although it may make such a disclosure if the witness in question or the person who disclosed or provided the information or document consents.[110] It is also prohibited from disclosing the fact that any information, document or identity has been disclosed.[111] The Tribunal cannot compel any person to give evidence at an oral hearing.[112]

9.51 Complainants in a recent matter submitted that these departures from normal adversarial procedures result in an inequality of arms in breach of the European Convention on Human Rights. They submitted that:

> The Tribunal receive information and documents from the Respondents without the complainants having any right to see the material or to cross examine on it. The same applies to information and opinions received by the Tribunal from a Commissioner. The Rules prevent the Tribunal, as a judicial body, from making their own assessments of what is necessary and proportionate. The Tribunal should be able to decide for themselves whether fairness requires disclosure of information and documents and the compelling of a witness to give oral evidence.[113]

9.52 The Tribunal held that the Investigatory Powers Tribunal Rules 2000 preventing complainants or others from obtaining access (either directly or indirectly via proceedings in the Tribunal) to sensitive information, documents or evidence in the hands of

---

107 *Regulation of Investigatory Powers Act 2000* (UK), s 69(4).

108 Such a procedure is an example of secret hearings, which are discussed more fully at [9.94]–[9.110] below. Rule 9(4) allows the Investigatory Powers Tribunal to hold separate oral hearings, (ie, without the attendance of the other party) where, for example, the person who is the subject of a complaint may be required to attend, make representations, give evidence and call witnesses.

109 *Investigatory Powers Tribunal Rules 2000* (UK), rule 6(2)(a) and 6(3)(a).

110 Ibid, rule 6(2)(b) and 6(3)(b).

111 See Ibid, rule 6(e).

112 Ibid, rule 11(3).

113 *In the Investigatory Powers Tribunal In Camera—In the Matter of Applications Nos IPT/01/62 and IPT/01/77—Draft Rulings of the Commission on Preliminary Issues of Law*, 23 January 2003, [179].

the security and intelligence services are compatible with Article 10 of the European Convention on Human Rights.[114] The Tribunal stated:

> The Rules protecting such information from being disclosed in Tribunal proceedings are necessary in the interests of national security, and, in particular, for the maintenance of the [neither confirm nor deny] policy and they are a proportionate interference under Article 10(2).[115] …
>
> The disclosure of information is not an absolute right where there are competing interests, such as national security considerations, and it may be necessary to withhold information for that reason, provided that, as in the kind of cases coming before this Tribunal, it is strictly necessary to do so and the restriction is counterbalanced by judicial processes which protect the interests of the Complainants: see *Fitt v United Kingdom* (2000) 30 EHRR 480 paras 45 and 46 and *R v Smith* (2001) 1 WLR 1031 at para 25.[116]

Immigration cases

9.53 Immigration is a key area where hearings may be held in a court or a tribunal in the absence of the party affected, or where evidence which is otherwise received by a court or tribunal is not disclosed to the party affected. The discussion below considers the position in Australia, the UK, Canada, New Zealand and to a limited degree the United States.[117]

Australia

9.54 The *Migration Act 1958* (Cth) allows certain information to be withheld from an applicant in relation to a decision that is under review before the Migration Review Tribunal (MRT). The withholding of information is based on ministerial opinion or certification about the nature of the information to be withheld. The Act provides in general terms that the MRT must give an applicant particulars of any information that the MRT considers would be a reason for affirming a decision under review to 'ensure, as far as is reasonably practicable, that the applicant understands why it is relevant to the review' and 'invite the applicant to comment on it.'[118] However, the MRT's obligations in this regard do not apply to 'non-disclosable information',[119] which is defined as information or matter:

> (a) whose disclosure would, in the Minister's opinion, be contrary to the national interest because it would:
>
> (i) prejudice the security, defence or international relations of Australia; or

---

114 Article 10 of the European Convention on Human Rights is set out in Appendix 3.

115 *In the Investigatory Powers Tribunal In Camera—In the Matter of Applications Nos IPT/01/62 and IPT/01/77—Draft Rulings of the Commission on Preliminary Issues of Law*, 23 January 2003, [124].

116 Ibid, [182].

117 The position in the United States is further considered under the heading 'Secret hearings' as, in some of those cases, the fact that such a hearing is taking place is also kept from the public.

118 See *Migration Act 1958* (Cth), s 359A(1).

119 Ibid, s 359A(4).

(ii) involve the disclosure of deliberations or decisions of the Cabinet or of a committee of the Cabinet; or

(b) whose disclosure would, in the Minister's opinion, be contrary to the public interest for a reason which could form the basis of a claim by the Crown in right of the Commonwealth in judicial proceedings; or

(c) whose disclosure would found an action by a person, other than the Commonwealth, for breach of confidence;

and includes any document containing, or any record of, such information or matter.[120]

9.55 Similarly, while the Act provides that an applicant is entitled to have access to any written material or a copy of any written material before the MRT for the purposes of a review, this entitlement is subject to a provision which allows for ministerial certification that disclosure of the information, other than to the MRT, would be contrary to the public interest.[121] Further, the Act provides that the Secretary shall not give to the MRT any document or information where the Minister has certified that it would be contrary to the public interest 'because it would prejudice the security, defence or international relations of Australia' or 'it would involve the disclosure of deliberations or decisions of the Cabinet or a committee of the Cabinet'.[122]

9.56 The *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) commenced on 15 July 2003, making amendments to the *Migration Act 1958*[123] encompassing the withholding of information from applicants and their lawyers, and also the withholding of information from the Federal Court and the Federal Magistrates Court. The amendments were designed to 'provide more effective protection to confidential information given to the Minister for the purposes of making decisions to refuse a visa application or to cancel an existing visa on the basis of the character or conduct of a non-citizen'[124] and to replace public interest immunity as the mechanism for protecting confidential information before the Federal Court and the Federal Magistrates Court.[125]

9.57 Prior to the amendments, s 503A of the *Migration Act 1958* provided in general terms that confidential information could not be disclosed unless the Minister made a written declaration after having consulted with the gazetted agency from which the

120 Ibid, s 5.
121 See Ibid, s 375A and s 362A(1).
122 Ibid, s 375. See also s 437, which is in similar terms except that it applies to the RRT. See also s 376 which deals with the MRT's discretion in relation to the disclosure of material certified by the Minister to be contrary to the public interest for reasons other than those specified in s 375.
123 Certain sections of the *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) came into effect on 16 July 2003: see *Migration Legislation Amendment (Protected Information) Act 2003* (Cth), s 2.
124 The Parliament of the Commonwealth of Australia, *Migration Legislation Amendment (Protected Information) Bill 2003—Revised Explanatory Memorandum*, 12 December 2002, [1].
125 Ibid, [4].

information originated.[126] The section did not protect confidential information provided by gazetted agencies from disclosure in proceedings before the Federal Court or the Federal Magistrates Court where a non-citizen contested a visa refusal or cancellation. The Minister and the Department of Immigration and Multicultural and Indigenous Affairs argued that:

> such proceedings have been prejudiced because there is no ability to bring before the court information supplied on a confidential basis by gazetted agencies and protect that information from disclosure to the noncitizen who is the subject of the visa cancellation. Indeed, it is suggested by the Minister and the department that some visa cancellations have been contested solely for the purpose of accessing the confidential information.[127]

9.58 Where a person commences court proceedings challenging an adverse character decision, the amendments:

> Limit the circumstances in which s 503A protected information can be disclosed to the Federal Court, or the Federal Magistrates Court;
>
> Enable the Federal Court and the Federal Magistrates Court to use interim and permanent non-disclosure orders to protect information that is disclosed to them; …
>
> Make it clear that the minister's power to make a declaration authorising the disclosure of confidential information under subsection 503A(3) of the act is a non-compellable power, and provide that the Federal Court and the Federal Magistrates Court have no power to review a decision by the minister not to exercise, or not to consider the exercise, of the power.[128]

9.59 The Federal Court and the Federal Magistrates Court may, on application by the Minister, in certain circumstances[129] make such orders as they think appropriate to ensure that, in the event that a declaration under s 503A(3) of the Act comes into force authorising the disclosure of confidential information to the Federal Court or the Federal Magistrates Court for the purposes of specified substantive proceedings and the information is disclosed, the information is not divulged or communicated to:

> (e) the applicant in relation to the substantive proceedings; or
>
> (f) the legal representative of the applicant in relation to the substantive proceedings; or

---

126 Gazetted agencies include Australian and overseas intelligence agencies.

127 Commonwealth, *Parliamentary Debates*, Senate, 26 June 2003, 12385 (Sen Sherry).

128 Ibid, 17 June 2003, 11666 (Sen Ian Campbell). *Migration Act 1958* (Cth), s 503A(3A) provides that the Minister does not have a duty to consider whether to exercise his or her power to make a declaration authorising the release of information.

129 Including where information is communicated to an authorised migration officer by a gazetted agency on condition that it be treated as confidential information and the information is relevant to the exercise of a power under specified sections of the Act dealing with the refusal or cancellation of a visa on character grounds and the information is relevant to specified substantive proceedings before the Federal Court or the Federal Magistrates Court and no declaration is in force under the Act authorising the disclosure of the information to the Court for the purposes of the substantive proceedings: see *Migration Act 1958* (Cth), s 503B(1).

(g) any other member of the public.[130]

9.60 In other words, if the Federal Court or the Federal Magistrates Court makes a non-disclosure order, it can rely on the confidential information for the purposes of the visa cancellation proceedings even though it is unable to disclose that information to anyone, including the non-citizen who is appealing the visa cancellation and that person's legal representatives.[131] If the court decides not to make such a non-disclosure order, the Minister can either adduce the evidence in the visa cancellation proceedings and the information can be supplied to the non-citizen applicant and his or her legal representatives, or the Minister can withdraw the information from the court's consideration, in which case the information will not be disclosed and cannot be relied upon by the court as evidence in the visa cancellation proceedings.[132]

9.61 The *Migration Act* sets out the matters to which the Federal Court or the Federal Magistrates Court must have exclusive regard in exercising their powers to make such orders, including:

(a) the fact that the information was communicated or originally communicated, to an authorised migration officer by a gazetted agency on the condition that it be treated as confidential information;

(b) Australia's relations with other countries;

(c) the need to avoid disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation and security intelligence;

(d) in a case where the information was derived from an informant—the protection of informants and of persons associated with informants;

(e) the protection of the technologies and methods used (whether in or out of Australia) to collect, analyse, secure or otherwise deal with, criminal intelligence or security intelligence;

(f) Australia's national security;

(g) the fact that the disclosure of information may discourage gazetted agencies and informants from giving information in the future;

(h) the effectiveness of the administration of justice; …[133]

9.62 The Attorney-General's Department has submitted that the *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) is a useful precedent for legis-

130 Ibid, s 503B(1). Examples of orders that the Federal Court or Federal Magistrates Court can make under subs (1) are set out in Ch 8 at [8.225] although the courts are not limited to making those orders: see *Migration Act 1958* (Cth), s 503B(3).

131 Commonwealth, *Parliamentary Debates*, Senate, 26 June 2003, 12385 (Sen Sherry).

132 Ibid.

133 *Migration Act 1958* (Cth), s 503B(5).

lation to protect classified and security sensitive information.[134] The ALRC's preliminary views on this are discussed in Chapter 10.

9.63 Secret evidence was led by the Australian Government and ASIO in the case of Zak Mallah, who was refused an Australian passport based on an adverse ASIO security assessment.[135] Mr Mallah appealed the decision not to renew his passport to the AAT. He and his lawyers were not permitted in an AAT hearing while counsel for the federal government gave evidence,[136] and his counsel could not be present to cross-examine the ASIO evidence.[137] Mr Mallah's counsel told the AAT:

> I am at a disadvantage in this case by not knowing the evidence and it's akin to boxing in the dark.[138]

9.64 In *Mohammed El Amer v Minister for Immigration, Local Government and Ethnic Affairs*, the applicants (a family) unsuccessfully challenged, under the *Administrative Decisions (Judicial Review*) *Act 1977* (Cth), the decision of an immigration officer to refuse their applications for visas. The refusal was based on adverse ASIO security assessments that indicated that the first applicant (the husband and father of the family) could be a threat to the national security of Australia. The applicants' basic premise was that they were denied access to the ASIO security assessments or were not otherwise provided with sufficient information about their contents to enable them to respond to any adverse statements contained in them.[139] Counsel for the applicants sought an order that he be allowed to inspect the security assessments. Lockhart J refused that application.

> For the Court not to disclose evidence to a party who may be affected by it, and to decline to disclose it on a restricted basis to counsel or solicitors for that party is a serious step which is taken only when necessary. … In my opinion, having carefully considered submissions of counsel, the competition between the interests of justice to the applicants on the one hand and the interests of national security on the other calls for the documents not to be disclosed to counsel for the applicant or any other person on behalf of the applicant. …
>
> There is no perfect solution to a problem such as has arisen here. For the Court not to have inspected the documents would have placed the applicants in an invidious

---

134 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

135 In December 2003, Zak Mallah became the first person to be charged under Commonwealth anti-terrorism laws. He has been charged with planning a terrorist act, which carries a maximum penalty of life imprisonment: 'Police Lay First Terror Charges', *The Canberra Times*, 5 December 2003, 7.

136 L Milligan, *Secret Hearing for Muslim's Passport Fight*, The Australian, <www.theaustralian.news.com.au/printpage/0,5942,6107547,00.html> at 11 March 2003.

137 L Morris, *Case against Muslim Youth*, The Sydney Morning Herald, <www.smh.com.au/articles/2003/03/10/1047144923803.html> at 11 March 2003.

138 As reported in L Milligan, *Secret Hearing for Muslim's Passport Fight*, The Australian, <www.theaustralian.news.com.au/printpage/0,5942,6107547,00.html> at 11 March 2003.

139 *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 2)* (Unreported, Federal Court of Australia, Lockhart J, 19 December 1989), 8–9.

> position. At least they have the comfort of the fact that a judge has inspected them and reached the view which I have indicated. … [140]
>
> The applicants have … the safeguard of the judicial eye having been cast over the security assessments of ASIO to ensure that the claim for secrecy with respect to them is not fatuous or otherwise without foundation.[141]

9.65 Asylum seekers in Australia who are permitted to apply for protection visas[142] must satisfy, among other things, public interest criterion 4002 (found in the *Migration Regulations 1994* (Cth)), which requires the applicant to be assessed by the competent Australian authorities as not directly or indirectly a risk to national security.[143] ASIO carries out the security assessments to which public interest criterion 4002 refers.

9.66 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.[144] 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.'[145] 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.[146] Mr Sultan made a fresh application for a protection visa, which was granted.

---

140 *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 1)* (Unreported, Federal Court of Australia, Lockhart J, 18 December 1989), 2–3.

141 *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 2)* (Unreported, Federal Court of Australia, Lockhart J, 19 December 1989), 10. Lockhart J inspected the documents notwithstanding that Sheppard J had previously inspected them on a return of subpoena issued at the request of the applicants and made a ruling upholding a claim for privilege in respect of those documents. Lockhart J stated that his inspection was warranted as the issues that faced him as trial judge were different from the issues facing Sheppard J on the return of subpoena. Lockhart J stated that he did not rely on anything in the ASIO security assessments to make any adverse findings of fact or to form any adverse impressions of the first applicant. *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 1)* (Unreported, Federal Court of Australia, Lockhart J, 18 December 1989), 4 and *Amer v Minister for Immigration, Local Government and Ethnic Affairs (No 2)* (Unreported, Federal Court of Australia, Lockhart J, 19 December 1989), 9, 10.

142 Including persons who have arrived in Australia on valid temporary visas and then invoke Australia's protection obligations.

143 *Migration Regulations 1994* (Cth), Sch 4, Pt 1, 4002.

144 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.

145 *Director General, Security v Sultan* (1998) 90 FCR 334, 335.

146 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.

9.67 Generally, the decision maker is not made aware of the actual information upon which ASIO has based its adverse security assessments.[147] There is no requirement that ASIO disclose adverse material to the applicant,[148] but procedural fairness requires, so far as is consistent with the requirements of security, the subject of a security assessment to be given an opportunity to reply to adverse matters.[149]

9.68 The Law Society of New South Wales submitted that:

> It is critically important that some means be available for review of all aspects of security assessments made in immigration or similar cases where the result can be that the person, the subject of that assessment, if adverse, may be removed from Australia. That review must involve the reviewer evaluating for himself or herself the seriousness of the danger posed by the applicant as well as the proportionality between the danger to Australian security which might be averted by the removal of the person and the danger to which that person might then be exposed. The Security Appeals Division of the Administrative Appeals Tribunal already has a similar role and, as a result, is equipped for this purpose. It may however be that the likely workload of extending a review within that Division to a wider range of assessments would be too great for it alone to handle and that it would be necessary to establish similar Divisions within the Refugee Review Tribunal and the Migration Review Tribunal. Any decision made should be subject to judicial review in a similar way to any other decision of these tribunals.[150]

9.69 The Law Council of Australia expressed concern about the 'potentially prejudicial use of classified information in immigration cases', stating that:

> The Council believes that [the use of such evidence] may result in erroneous evidence remaining unchallenged and unchallengeable by the applicant, with very grave consequences. Although in some cases, sustained protest can lead to an internal inquiry by the Director-General of Security of the particular risk assessment, this would be exceptional. The question is whether the AAT should be able to receive such evidence and decide, as does a court, whether to disclose the material or to make protective orders.[151]

9.70 The ALRC is of the preliminary view that there is a legitimate concern in relation to the use of security assessments in immigration matters. However, any reform in relation to security assessments in immigration matters would be better dealt with in the context of a broader enquiry into protection visas. It is difficult for the ALRC to make a proposal in this area without considering the broader context, and in

---

147 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]; and Commonwealth, *Parliamentary Debates*, House of Representatives, 6 February 2001, 24015 (Philip Ruddock, Minister for Immigration and Multicultural Affairs).

148 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.

149 Advisory Committee member, *Notes*, 19 September 2003.

150 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.

151 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

the absence of any submissions from key stakeholders such as the Department of Immigration, ASIO, the RRT, the MRT, and human rights and civil liberties groups.

United Kingdom

9.71 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 (ECHR) against the British government in *Chalal v The United Kingdom*.[152] The ECHR 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.[153] 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.[154]

9.72 The *Special Immigration Appeals Commission Act 1997* (UK) allows rules to be made enabling the Special Immigration Appeals Commission (SIAC) to hold proceedings in the absence of any person, including the appellant and any legal representative appointed by him or her,[155] having regard in particular to the 'need to secure that infor-

---

152 *Chalal v The United Kingdom* (1996) European Court of Human Rights No 70/1995/576/662.

153 See L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), 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.

154 L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994), 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.

155 *Special Immigration Appeals Commission Act 1997* (UK), s 5(3)(b).

mation is not disclosed contrary to the public interest.'[156] The Act also allows rules to be made enabling the SIAC to give the appellant a summary of any evidence taken in his or her absence.[157] 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.[158] Appointed lawyers are not responsible to the person whose interests they are appointed to represent.[159]

> 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.[160]

9.73 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 SIAC but objects to it being disclosed to the appellant or his or her representative.[161] Amnesty International has expressed particular concern about the SIAC's procedures in relation to its reviews of whether people are 'suspected international terrorists'—and as a consequence subject to detention, deportation or exclusion from refugee status:

> the person concerned should be entitled to see and challenge all the evidence used to determine whether they are a 'national security risk' or a 'suspected international terrorist'.[162]

9.74 Evidence can also be withheld from a person under the *Nationality, Immigration and Asylum Act 2002* (UK). Under that Act, immigrants holding dual nationality may be stripped of British citizenship if they have done anything 'seriously prejudicial' to the 'vital interests of the United Kingdom or a British overseas territory'. A person who is given notice of a decision to deprive him or her of citizenship may appeal

---

156 Ibid, s 5(6)(b).

157 Ibid, s 5(3)(d).

158 Ibid, s 6(1).

159 Ibid, 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.

160 See the United Kingdom Parliament website at <www.parliament.the-stationery-office.co.uk/pa/cm200102/cmselect/cmhaff/351/351ap20.htm>.

161 See *Special Immigration Appeals Commission (Procedure) Rules 2003* SI No 1034 (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 SIAC 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 SIAC, 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.'

162 Amnesty International, *Rights at Risk: Amnesty International's Concerns regarding Security Legislation and Law Enforcement Measures* (2002), 31.

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.[163]

9.75 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 on 11 September 2001. Al-Masri was the first person targeted under the new powers.[164] 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, criticised the administrative nature of the decision, arguing that:

> Any decision to strip someone of citizenship should be for a court, based on evidence of treason or similarly serious offences.[165]

Canada

9.76 The *Immigration and Refugee Protection Act 2001* (Canada) provides for the leading of secret evidence.[166] Under the Act, the Minister of Citizenship and Immigration and the Solicitor General may certify that a permanent resident or a foreign national is inadmissible on grounds including the threat to security. The certificate is referred to the Federal Court for determination[167] and, if the Court determines that the certificate is reasonable, it automatically becomes a removal order. In considering the matter:

> (b) the judge[168] shall ensure the confidentiality of the information[169] on which the certificate is based and of any other evidence that may be provided to the judge

---

163 *Nationality, Immigration and Asylum Act 2002* (UK), s 4 amending the *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.

164 S O'Hanlon, *Radical Cleric Hamza Faces Dual Threat*, <http://uk.news.yahoo.com/030406/80/dx3oa.html> at 6 April 2003.

165 J Hopps, *Blunkett Targets 'Un-British' Immigrants*, <http://uk.news.yahoo.com/030401/80/dwqd1.html> at 1 April 2003.

166 *Immigration and Refugee Protection Act 2001* (Canada) became law on 28 June 2002, replacing the *Immigration Act 1976* (Canada). Section 40.1 of the former Act permitted the presentation of evidence in a hearing closed to the person affected and his or her lawyer.

167 See Ibid, s 77(1).

168 'Judge' means the Associate Chief Justice of the Federal Court or a judge of the Trial Division of that Court designated by the Associate Chief Justice: Ibid, s 76.

169 'Information' means 'security or criminal intelligence information and information that is obtained in confidence from a source in Canada, from the government of a foreign state, from an international organization of states or from an institution of either of them': Ibid, s 76.

> if, in the opinion of the judge, its disclosure would be injurious to national security or to the safety of any person; …
>
> (d) the judge shall examine the information and any other evidence in private within seven days after referral of the certificate for determination;
>
> (e) on each request of the Minister or the Solicitor General of Canada made at any time during the proceedings, the judge shall hear all or part of the information or evidence in the absence of the permanent resident or the foreign national named in the certificate and their counsel if, in the opinion of the judge, its disclosure would be injurious to national security or to the safety of any person;
>
> (f) the information or evidence described in paragraph (e) shall be returned … and not be considered by the judge in determining whether the certificate is reasonable if … the judge determines that the information or evidence is not relevant or, if it is relevant, that it should be part of the summary;
>
> (g) the information or evidence described in paragraph (e) shall not be included in the summary but may be considered by the judge in deciding whether the certificate is reasonable if the judge determines that the information or evidence is relevant but that its disclosure would be injurious to national security or to the safety of any person;
>
> (h) the judge shall provide the permanent resident or the foreign national with a summary of the information or evidence that enables them to be reasonably informed of the circumstances giving rise to the certificate, but that does not include anything that in the opinion of the judge would be injurious to national security or to the safety of any person if disclosed;
>
> (i) the judge shall provide the permanent resident or foreign national with an opportunity to be heard regarding their inadmissibility; … [170]

9.77 The Minister may also seek the non-disclosure of information during an admissibility hearing, a detention review or an appeal before the Immigration Appeal Division of the Immigration and Refugee Board, in which case the above provisions apply to the determination of the application 'with any modifications that the circumstances require, including that a reference to 'judge' be read as a reference to the applicable Division of the [Immigration and Refugee] Board.'[171] Accordingly, secret evidence may be led in such proceedings where the Board is of the opinion that its disclosure would be injurious to national security.

9.78 Justice James K Hugessen, a Canadian Federal Court judge before whom secret trials have been conducted, has expressed his concern about the process:

---

170 Ibid, s 78.

171 Ibid, s 86. See also s 87 which provides for the Minister, in the course of a judicial review, to make an application to the judge for the non-disclosure of certain information, including information protected under s 86(1). The provisions of s 78 (set out, in part, at [9.76] above) apply to the determination of the application (except for the provisions relating to the obligation to provide a summary and the time limit referred to in s 78(d)) with any modifications that the circumstances require: *Immigration and Refugee Protection Act 2001* (Canada), s 87(2).

> All the national security functions which are laid on the Federal Court have this in common: they involve at one stage or another and sometimes throughout the whole piece a judge of the Court sitting alone in what are called hearings, but they are held in the absence of one of the parties. That is to say ex parte so that the judge may, if he or she sees fit, take communication of the evidence, the information which is said to be too sensitive to be allowed to be revealed to the person concerned and not only evidence, but also argument which may rely on evidence or may deal with matters which may be too sensitive to be revealed to the public.
>
> This is not a happy posture for a judge … We do not like this process of having to sit alone hearing only one party and looking at the materials produced by only one party and having to try to figure out for ourselves what is wrong with the case that is being presented before us and having to try for ourselves to see how witnesses that appear before us ought to be cross-examined.
>
> … good cross-examination requires really careful preparation and a good knowledge of your case. And by definition, judges do not do that. We do not get to prepare our cases because we do not have a case and we do not have any knowledge except what is given to us and when it is only given to us by one party we are not well suited to test the materials that are put before us.
>
> … it might be helpful if we created some sort of system somewhat like the public defender system where some lawyers are mandated to have full access to the CSIS files, the underlying files, and to present whatever case they could against the granting of the relief sought.[172]

United States

9.79 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.'[173] 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.[174]

9.80 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

---

172 *Immigration and Refugee Protection Act*, Victoria Independent Media Center, <http://victoria.indymedia.org/print.php?id=14538> at 25 May 2003. The comments were reportedly made by Justice Hugessen at a conference in Montreal in 2002.

173 Secret Evidence Repeal Bill 2001 (USA).

174 K Snyder, 'A Clash of Values: Classified Information in Immigration Proceedings' (2002) 88(2) *Virginia Law Review* 447, 472.

probably derailed the proposed legislation, which would have augmented procedural protections for aliens.[175]

9.81 The Alien Terrorist Removal Court (ATRC) was established in 1996,[176] modelled on the special court created by the *Foreign Intelligence Surveillance Act* (discussed at [9.102] below). 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 whom the US 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.

9.82 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.[177] However, the normal court requirement to produce evidence could expose and endanger intelligence sources.[178]

9.83 Where the Attorney General has classified information that an alien is a terrorist, he or she may seek removal of that alien by filing an application under seal with the ATRC. The application is submitted ex parte and in camera.[179] Where the application is approved by the ATRC, deportation proceedings are commenced. These proceedings are open to the public.[180] The alien must be given reasonable notice of the deportation proceedings, the nature of the charges and a general account of the basis of the charges.[181] The alien has a right to be present at the hearing and to be represented by counsel.[182] However, the alien is not entitled to have access to classified information. The judge of the ATRC is to examine ex parte and in camera any evidence, the disclosure of which the Attorney General has determined would pose a risk to national security or to a person's security because it would disclose classified information. The alien and the public are not to be informed of this evidence or its sources, except that the alien is entitled to an unclassified summary of the specific evidence that does not pose that risk.[183] The judge must approve the summary if he or she finds that it is sufficient to enable the alien to prepare a defence.[184]

---

175 Ibid, 450.

176 8 USC (US), s 1532 (1996).

177 The non-citizens (or aliens) may be deported even if they are legally residing in the US.

178 B Wittes, *Does the US Really Need its New Secret Tribunal?*, Slate, <http://slate.msn.com/id/2129/> at 12 May 2003.

179 8 USC (US), s 1533(a)(1) and (a)(2)(1996).

180 Ibid, s 1534(a)(1) and (a)(2) (1996).

181 Ibid, s 1534(b)(1) and (b)(2) (1996).

182 Ibid, s 1534(c)(1).

183 Ibid, s 1534(3)(A) and (3)(B).

184 Ibid, s 1534(3)(C). If the ATRC does not approve the summary, the Government has 15 days to correct the deficiencies identified by the court and to submit a revised summary. If the revised summary is not approved by the court within 15 days of its submission, the deportation proceedings are to be terminated unless the judge finds that either the 'continued presence of the alien in the United States would likely cause serious and irreparable harm to the national security or death or serious bodily injury to any person' and the provision of the summary would cause similar harm or injury. See 8 USC (US), s 1534(D)(i)–(iii). If a judge makes such a finding, the Department of Justice is to have a statement delivered to the

9.84 The US Department of Justice has argued that it has been placed in a difficult position. 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.[185] 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.[186]

New Zealand

9.85 Part 4A of the *Immigration Act (1987)* (NZ) provides for special procedures in cases involving security concerns, including reliance on secret evidence. The objects of the Part include a recognition that classified security information held by the New Zealand Security Intelligence Service should be protected in its use under the Act or in any proceedings which relate to its use;[187] and that ascertaining the balance between the public interest and the protection to be given to an individual affected by the use of the information is best achieved by having an independent person of high judicial standing consider the information and approve its proposed use.[188]

9.86 The Director of Security may withhold certain classified security information if, in the Director's opinion, it 'cannot be divulged to the individual in question or to other persons' because of the particular specified character of the information[189] and the fact that its disclosure would be likely to have a particular specified effect, such as prejudicing the security or defence of New Zealand or the international relations of the Government of New Zealand.[190] The Director of Security can provide a security risk certificate to the Minister of Immigration if he or she holds credible classified security information in respect of an individual who is not a New Zealand citizen in respect of whom decisions can be made under the Act and who meets a relevant security criterion specified in the Act.[191] The Minister of Immigration may make a preliminary decision to rely on the certificate.[192] Review proceedings cannot be taken in any court in respect of the certificate or the Director of Security's decision to issue the certificate.[193]

---

alien that no summary is possible, and the classified information submitted in camera and ex parte may be used: see s 1534(E)(ii).

185 S Valentine, *Flaws Undermine Use of Alien Terrorist Removal Court*, Washington Legal Foundation, <www.prestongates.com/publications/article.asp?pubID=259> at 12 May 2003.

186 Ibid.

187 See *Immigration Act 1987* (NZ), s 114A(a) and (b).

188 See Ibid, s 114A(c) and (d).

189 See Ibid, s 114B(1)(a). For example, the information might provide details of operational methods available to the New Zealand Security Intelligence Service or operations proposed to be undertaken by it.

190 See Ibid, s 114B(1)(b).

191 See Ibid, s 114D(1). For example, a relevant refugee removal security criterion is that 'there are reasonable grounds for regarding the person as a danger to the security of New Zealand, in terms of Article 33.2 of the Refugee Convention': see *Immigration Act 1987* (NZ), s 114C(5)(a).

192 See *Immigration Act 1987* (NZ), s 114G. A person in New Zealand in respect of whom a security risk certificate has been issued and upon which the Minister of Immigration has made a preliminary decision to rely upon, must be served by the police with a notice to that effect, which also specifies the relevant security criterion or criteria to which the certificate relates, the potential effect of the certificate and the rights of the person, including the right to review. Where the person has been served such a notice by a

9.87 A person who is notified that the Minister has made such a decision can seek a review by the Inspector-General of Intelligence and Security or the Director of Security's decision to issue the security risk certificate.[194] A person who seeks review is allowed access, to the extent provided by the *Privacy Act 1993* (NZ), to any information about him or herself other than the classified security information.[195] On a review, the Inspector-General must determine whether:

> (a) The information that led to the making of the certificate included information that was properly regarded as classified security information; and
>
> (b) That information is credible having regard to the source or sources of the information and its nature, and is relevant to any security criterion; and
>
> (c) When a relevant security criterion is applied to the person in light of that information, the person in question is properly covered by that criterion—
>
> and thus whether the certificate was properly made or not.[196]

9.88 If the Inspector-General decides that the security risk certificate was properly made and the Minister of Immigration makes a decision to rely on the confirmed certificate,[197] certain consequences set out in the Act follow, including the immediate non-appellable and non-reviewable cancellation or revocation of any visa or permit that the person still holds, and the making of a deportation or removal order.[198] If the Inspector-General decides that the security risk certificate was not properly made, the person who sought the review must be immediately released from custody, and any immigration processing or appeal that was stopped as a result of reliance on the certificate immediately recommences.[199]

Consultations and submissions

9.89 The NSW Law Society has addressed a number of the questions raised by the ALRC in BP 8 in relation to the use of secret evidence,[200] submitting that:

> The taking of evidence in the absence of one or more parties should be permitted only in the most extraordinary circumstances, but never without notice to the excluded party or parties that such evidence is to be taken and used in the proceeding. The normal rules of evidence should apply if such secret evidence is taken. It should be a condition precedent to the taking of such evidence that the party leading that evidence

---

member of the police force, the police must arrest the person without warrant and place him or her in custody: see *Immigration Act 1987* (NZ), s 114G(4) and (5).

193 *Immigration Act 1987* (NZ), s 114H(4).

194 Ibid, s 114H(1).

195 Ibid, s 114H(2)(b).

196 Ibid, s 114I(4).

197 See Ibid, s 114K(1) and (2).

198 See Ibid, s 114K, in particular, s 114K(4). A person may, with the leave of the Court of Appeal, appeal to the Court of Appeal, where he or she is dissatisfied with the decision of the Inspector-General to confirm the security certificate on the ground of being erroneous in law: *Immigration Act 1987* (NZ), s 114P.

199 See *Immigration Act 1987* (NZ), s 114L.

200 See Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 33, 35, 36, 37, 39 and 40.

> will provide at its expense an independent counsel to represent any absent party's interest who may, of right, object to the omission of any evidence, cross examine and make submissions on any aspect of the secret evidence. If the taking of secret evidence is to be permitted for reasons of national security, a certificate should be provided (the giving of which should be subject to review similar to such a certificate given under the *Freedom of Information Act 1982* (Cth)). A record in such form and subject to such access conditions as the presiding judicial officer or decision maker finds necessary in the circumstances should be kept of any secret evidence taken.[201]

9.90 HREOC has submitted that measures could be taken to protect witnesses and classified information in criminal matters without resorting to secret evidence and secret hearings.[202] It noted the concession made by the ECHR that the right of a defendant to call witnesses and to cross-examine witnesses against him or her are not absolute rights where there is a compelling reason for encroaching on these rights.[203] HREOC also submitted that where a defendant is denied these rights, 'the arrangements must be the least adverse to the defendant as is possible in the circumstances, and the evidence given under these special arrangements should not be the major item in the case against the defendant' and that 'wherever the rights of the defendant are diminished there should be some compensating protection.'[204]

9.91 Victoria Legal Aid submitted that 'at no stage should the defendant's legal representative be refused permission to attend when evidence is being tendered' and that records of any secret proceedings should be kept.[205]

9.92 The Attorney-General's Department has submitted that:

> In some instances it may be appropriate to develop "special evidence procedures" for determining the admissibility of evidence, for example, a closed hearing on admissibility alone. If this is necessary some fundamental safeguards should apply. At all times the court must be given unfettered access to the evidence in question in order to make an appropriate determination of its admissibility. While the exclusion of a party may be appropriate in some instances, this should only be done in the most extreme cases and the party must always be represented by counsel with full knowledge of the case.[206]

9.93 The ALRC's preliminary views on secret evidence in court and tribunal proceedings are set out in Chapter 10.

---

201 Law Society of New South Wales, *Submission CSSI 9*, 28 August 2003.
202 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003.
203 *Van Mechelen v The Netherlands* (1997) III Eur Court HR 691, [52]–[53]. See the discussion of this case in Ch 7.
204 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003. See also the discussion of *Van Mechelen v The Netherlands* (1997) III Eur Court HR 691 in Ch 7.
205 Victoria Legal Aid, *Submission CSSI 14*, 26 September 2003.
206 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

Secret hearings

Immigration

9.94 In some cases, even the fact that a hearing is taking place is shrouded in secrecy. Certain immigration hearings in the United States after September 2001 have been conducted in accordance with special procedures. The US Department of Justice broke with a long-established practice of open immigration hearings when it closed proceedings for people detained by the US Immigration and Naturalization Service (INS) after 11 September 2001,[207] arguing that open hearings of detainees could compromise terrorism-related investigations.

9.95 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[208] setting out 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. …[209]

9.96 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.

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

> Unsubstantiated speculations about potential damage to the government's investigation … should not be permitted to override the fundamental principle that arrests

---

207 In July 2002, in response to a Congressional request for information, the US Department of Justice stated that, as at 29 May 2002, 611 people had been subject to secret hearings and that 419 of them had more than one secret hearing: Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), 25.

208 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.

209 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.

> and hearings affecting a person's liberty should be public to ensure fairness and to prevent abuse of power. …
>
> 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. …
>
> 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.[210]

9.98 A three-judge panel of the US Court of Appeals for the 6th Circuit subsequently held Judge Creppy's directive to be an infringement of the First Amendment right of access.[211] The Court of Appeals held that there was a First Amendment right of access to deportation proceedings[212] 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.[213] 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.[214] The Court of Appeals found that, while the Government's on-going anti-terrorism investigation provided a compelling interest, Judge Creppy's directive was not narrowly tailored[215] and did not require particularised findings.[216] 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

---

210 Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), 5, 7, 30.

211 *Detroit Free Press v Ashcroft* (Unreported, 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.'

212 Ibid, 15.

213 Ibid, 19.

214 Ibid, 19.

215 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.

216 Ibid, 19.

> 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.[217]

9.99 The Court of Appeals identified the following values inherent in maintaining open proceedings:[218]

> 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'.[219]
>
> 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'.

9.100 However, the decision of the US Court of Appeals for the 3rd Circuit in *North Jersey Media Group v John Ashcroft*[220] is at odds with that of the 6th Circuit. The 3rd Circuit held that the press and the 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.[221]

9.101 On 27 May 2003, the US Supreme Court declined to review the decision of the 3rd Circuit Court of Appeals, leaving in place conflicting precedents about the US Government's right to conduct secret immigration hearings.[222]

---

217 Ibid, 2.
218 Ibid, 18–19.
219 *Richmond Newspapers, Inc v Virginia* 448 US 555 (1980), 571.
220 *North Jersey Media Group Inc v John Ashcroft, Attorney General of the United States, and Michael Creppy, Chief Immigration Judge of the United States* (Unreported, US Court of Appeals for the 3rd Circuit, Becker CJ; Scirica and Greenburg JJ, 8 October 2002).
221 Ibid, 35.
222 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>.

Specialist courts

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

9.103 The FISC is composed of seven Federal District Court judges appointed on 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.[223]

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

(a) 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;

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

(c) there is no provision for certification that the surveillance was conducted according to the warrant.[224]

9.105 In 2002, the FISA Review Court[225]—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[226]—meaning that the Government must show probable cause that an individual is committing, is about to commit or has committed a crime.[227] 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 Amend-

223 *Foreign Intelligence Surveillance Act 1978* (USA), 36 USC, s 1802–1804 (1978).

224 See the Electronic Frontier Foundation: <www.eff.org/Privacy/Surveillance/Terrorism_militias/fisa_faq.html>.

225 This court was established as part of the original Act in 1978 but had never sat until 2002.

226 F Murray, *High Court Rejects Challenge to Spy Laws*, The Washington Times, <www.washtimes.com/national/20030325-284477.htm> at 25 March 2003.

227 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.' See also Appendix 3.

ment protections given the important government interest in national security.[228] In March 2003, the US Supreme Court rejected a challenge to that ruling by the American Civil Liberties Union.[229]

Consultations and submissions

9.106 In BP 8, the ALRC asked whether the fact that a hearing is taking place, even if closed to the public and to one or more parties or their legal representatives, should ever be withheld from the parties affected or from the public.

9.107 The Australian Press Council submitted:

> While there may be some instances where *in camera* hearings are appropriate, the conduct of hearings in secret is so antithetical to notions of justice and accountability that it should be considered entirely unacceptable. There may be some basis for filtering information which is released to the public about proceedings, such as the identities of parties or the content of evidence, but the public have a right to know that the proceedings are taking place. …
>
> In the event that proceedings be held … in secret, it is crucial that the proceedings be recorded and copies of all evidence tendered be retained.[230]

9.108 The ALRC was informed that the fact that a hearing has taken place is sometimes suppressed for a period of time. This might occur, for example, to avoid prejudicing an on-going investigation, or to protect an informant.[231]

9.109 The ALRC's preliminary view is that the fact that a hearing is taking place should never be kept from the party whose rights or interests are being determined or affected by the hearing, whether that hearing is in a court or a tribunal. Of course, hearings in relation to applications for search warrants and applications for approval to adopt other investigative tools would not be covered by this proposal, as obviously any investigative forensic benefit could be lost or diminished if the party affected were put on notice of such a hearing.[232]

9.110 It should be left to the discretion of the court or tribunal whether there is a need to keep the fact of the hearing secret from the public for a temporary period for any public interest reasons, such as protection of an informant. Permanent suppression from the public of the fact that a hearing has taken place should not be allowed other than in exceptional circumstances. Whenever the fact of a hearing is suppressed, tran-

---

228 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> at 12 May 2003.

229 F Murray, *High Court Rejects Challenge to Spy Laws*, The Washington Times, <www.washtimes.com/national/20030325-284477.htm> at 25 March 2003.

230 Australian Press Council, *Submission CSSI 17*, 5 December 2003.

231 Director of Public Prosecutions for Victoria, *Consultation*, Melbourne, 29 August 2003.

232 See also discussion in Ch 7 at [7.41] where a distinction is drawn between public scrutiny of investigative procedures and public scrutiny of other court hearings.

scripts of the proceedings should be made and retained. The ALRC's proposals in this regard are set out in Chapter 10.

10. Proposals for Reform—Courts and Tribunals

Contents

10.1 This chapter sets out the ALRC's proposals concerning the use of classified and security sensitive information in court, tribunal and similar proceedings. It summarises the statements of principle found in Chapters 8 and 9, and seeks to bring those principles together in a single, coherent set of proposals relating to the use of classified and security sensitive information in legal proceedings.

A new statute

10.2 In BP 8, the ALRC asked whether Australia needs a statute or other provisions setting out a procedural framework for the disclosure and admission of classified and security sensitive information in court and tribunal proceedings, fulfilling a similar role to the *Classified Information Procedures Act* (USA) (CIPA).[1] The procedural framework set out in CIPA is discussed in Chapter 8 of this Discussion Paper.

10.3 The ALRC's current view is that a statutory regime is the best solution, and in general terms this proposal has received support in consultations and from the

1 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 47.

Advisory Committee. The use of CIPA as a model, at least in some respects, also received support. This Chapter discusses the proposed regime in detail. It is intended to cover both criminal and civil proceedings, all courts governed by the regime,[2] and all federal tribunals. It is intended to apply only to cases where classified or sensitive national security information will arise, and is not intended to form part of the statutes that relate to the procedural and evidentiary rules governing Australian federal courts or Australian courts generally. The Proposals in this Chapter are intended to establish the general principles that would, if adopted, govern the drafting of the new statute and the court rules and regulations that the courts and tribunals themselves would need to prepare in order to give effect to the overall statutory intent.

10.4 In reaching this preliminary conclusion, the ALRC considered a number of options. For example, it had been mooted that a formal statutory regime might not be necessary and that it could be left to the courts themselves to determine new rules governing their own procedures in line with certain statements of principle. However, this found little favour in consultations; the ALRC was told that the importance of the classified and security sensitive information under consideration warranted a regime with statutory force, and that it was insufficient, especially in the area of national security, to rely solely on general guidelines to the courts, or to leave it to each of the courts to reform their statutes and procedures.[3]

10.5 A statute applying in all Australian courts, or at least in all federal courts, would also serve to standardise procedures, or would at least assist in doing so.

10.6 However, balanced against the desire for consistency is the need for flexibility. One purpose of the ALRC's Proposals is to ensure that courts and tribunals have an appropriately supple system at their disposal to allow them to deal with situations that can only be imperfectly foreseen. It is important that any regime adopted not be overly prescriptive, leaving the courts with the ultimate discretion to determine the procedures that will apply in any particular case in line with the specific circumstances and the dictates of justice. Accordingly, while the statements of principle found in the Proposals in this Chapter include a number of options, they do not purport to be exhaustive.

10.7 The ALRC considered two options for the location of the new statutory regime: either in the *Evidence Act 1995* (Cth) or in a new, separate Act. The Evidence Act option was attractive as it would avoid the creation of a new Act and would keep important legislative provisions governing the handling of evidence in one place. The *Evidence Act* generally applies to proceedings in all federal courts and the courts of the Australian Capital Territory.[4] Its substantive provisions are also mirrored in the *Evidence Act 1995* (NSW), so that many of the courts that are likely to handle espionage

---

2 See [10.9]–[10.13] below.

3 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003; Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

4 *Evidence Act 1995* (Cth), s 4(1).

cases, for example, are covered by this uniform legislation.[5] The *Evidence Act* does not apply in the courts of the other States and the Northern Territory, even when they exercise federal jurisdiction. Seeking to apply the *Evidence Act* in all courts exercising federal jurisdiction could, apart from any other problem, result in different laws applying to the handling of the same evidence in any case where both federal and state (or territory) jurisdiction were being exercised.

10.8 Ultimately, the ALRC has opted to propose that the new regime be placed in a dedicated Act. The ALRC is concerned that, albeit for good reasons in the public interest, this regime does authorise courts to depart in exceptional cases from fundamental standards of fair trials and open justice. It should only be used, therefore, in those exceptional cases. Once procedures diverging from standards that protect human and defendants' rights are introduced, there is a tendency for them to be applied in cases outside the exceptional range that warranted their adoption in the first place. The abridgement of human and procedural rights in order to suppress information in the interests of national security and defence should be used only in cases where that security and defence would suffer real harm if the usual practices of open justice and full disclosure of evidence were used. For that reason, the ALRC prefers to see the new regime in legislation separate from the *Evidence Act 1995* and other legislation dealing with court procedures generally, and to be given a title that emphasises the exceptional nature of the procedures it authorises, such as the National Security Information Procedures Act.

10.9 The ALRC has also had to consider the range of courts and proceedings in which the new regime would apply. Interestingly, s 5 of the *Evidence Act 1995* (Cth) applies certain specified provisions of the Act to all Australian courts (rather than just federal courts), with the result that there is national uniformity where they apply. These provisions are clearly based on express legislative powers granted to the Australian Parliament in the *Australian Constitution*, such as customs and excise, and the recognition of official records and documents.

10.10 If a regime governing the handling of classified and security sensitive information in courts and tribunals were based on one or more express heads of legislative power granted by the *Australian Constitution* to the Australian Parliament, the proposed regime could extend to all Australian courts, eliminating the possibility of inconsistent practice in different courts. A number of heads of legislative power come readily to mind:

- The naval and military defence of the Commonwealth and of the States, and the control of the forces to execute and maintain the laws of the Commonwealth;
- External affairs;

5 For example, Simon Lappas was prosecuted in the courts of the Australia Capital Territory.

- Postal, telegraphic, telephonic, and other like services;
- Naturalisation and aliens;
- Immigration and emigration;
- The influx of criminals;
- The control of railways with respect to transport for the naval and military purposes of the Commonwealth; and
- Matters incidental to the execution of any power vested by the *Australian Constitution* in the Australian Parliament, the Australian Government, the federal judicature or any Australian Government department or officer.[6]

10.11 To this list can be added matters referred by the States to the Australian Parliament.[7] This course was adopted in relation to recent anti-terrorism legislation to ensure that the Australian Parliament could pass comprehensive national laws. However, it would involve complex political negotiation among Australia's nine major governments and could not be guaranteed success.

10.12 The eight heads of power listed above—together with any inherent power that the Australian Government may have to legislate for the defence, security and integrity of the Commonwealth—would seem to cover all likely legal proceedings in which classified or sensitive national security information would arise. However, whereas the Australian Government inarguably has power to legislate to govern the procedure to be adopted in federal courts, reliance on these disparate heads of power to extend the proposed regime to all Australian courts might mean that there is some room to argue in marginal cases that the proposed regime does not apply. If it did not in some exceptional case, the existing common law and legislative powers would remain and could be relied on, if appropriate.

10.13 On balance, the ALRC considers that the new regime should be expressed to apply in all Australian courts notwithstanding the chance, apparently remote, that some marginal cases might fall outside its scope. It would apply without question in all federal courts and in what is likely to be the overwhelming majority of relevant cases where one or more of the heads of power listed above would support the legislation. If felt necessary, it might be possible to persuade state and territory governments to refer powers or pass complementary legislation to cover these marginal cases.

---

6 See *Australian Constitution* , s 51(vi), (xxix), (v), (xix), (xxvii), (xxviii), (xxxii) and (xxxix) respectively.
7 See Ibid, s 51(xxxvii).

Mechanisms before and during trial

10.14 In BP 8 and elsewhere in this Discussion Paper, a distinction has been made between mechanisms used by courts to restrict disclosure of classified and security sensitive information before and during trials. The ALRC's Proposals do not make this distinction and are intended to apply to all stages of proceedings otherwise covered by the new Act.

Criminal proceedings

10.15 In assessing the introduction in Australia of such a statute modelled at least in part on CIPA, it has to be borne in mind that that Act emanates from a jurisdiction that traditionally imposes higher burdens of disclosure on an accused person in criminal proceedings than in Australia. If a similar regime were introduced in Australia, there would be some concern that this would represent an erosion of an accused's rights. Some of the arguments that have been raised in the past in opposition to pre-trial disclosure by the defence (in contexts not specifically related to classified and security sensitive information) include that:

> Requiring the defendant to provide information about the defence case before trial would be inconsistent with the principle that the burden of proving the defendant's guilt is on the prosecution, which is required to establish guilt without any assistance from the defendant. Compulsory defence pre-trial disclosure might also operate in practice as a form of compulsion on the defendant, inconsistent with the defendant's privilege against self-incrimination. It is also argued that compulsory defence pre-trial disclosure would be inconsistent with the presumption of innocence.[8]

10.16 One way of addressing such concerns would be to circumscribe strictly the situations in which such an obligation arose on the part of an accused to reduce the possibility that there may be a consequent diminution of an accused's rights in other situations.

10.17 It must also be acknowledged that substantial inroads have already been made into an accused's rights in this area, especially with the passing of recent state pre-trial disclosure legislation, which is discussed below. Against this background, to extend an accused's obligations to provide pre-trial disclosure of the items of evidence relied upon by him or her that are of a classified or security sensitive nature would not necessarily represent a great departure from current practice. It would arise in a very small number of cases in a procedure where all steps are determined by the court seized of the matter, whose prime obligation is to ensure so far as it can that each matter proceeds in accordance with the requirements of justice peculiar to that case. Furthermore, a mechanism such as that set out in CIPA would have the benefit of providing a framework for the ventilation of issues relating to the disclosure and presentation of classified or security sensitive material well before trial. The admissibility of any such material, and the form (if any) in which it could be presented at trial, would be determined

8 NSW Law Reform Commission, *Discussion Paper 41—The Right to Silence*, <www.lawlink.nsw.gov.au/lrc.nsf/pages/dp41toc>, [4.62] (citations omitted).

at an early stage. For example, if in *Lappas*[9] the defence had been required to give formal pre-trial notification that it intended to rely upon the contents of certain classified documents, the Crown's claim for public interest immunity could have been dealt with prior to trial. Even if the ultimate outcome were to be that the Crown could not pursue any or some of the charges on the indictment, at least that would have been ascertained in advance with less disruption to the running of the trial itself. In this regard, the argument that compulsory pre-trial disclosure by the defence seems not to involve a fundamental breach of principles because 'the only difference between pre-trial disclosure and advancing a defence at trial [is] timing' has an element of persuasion.[10]

10.18 Material that the defence proposes to rely on that does not contain sensitive national security information would not have to be disclosed under the proposed regime, though other legislation and court rules might have an impact.

10.19 Requiring pre-trial disclosure by the defence of classified and security sensitive information in a spy case does not appear to present any major tactical disadvantages as both sides will generally know which information is likely to be in issue. The defence may want to rely on the classified information in an espionage case to show that the information was not damaging to national security. The prosecution could normally anticipate that in any event. It has also been suggested that, as the classified information is generally known to both parties in an espionage case, the defendant is more likely to enter a plea than in a terrorism case where the defence will not be privy to all of the classified information in the hands of the prosecution.[11]

10.20 It is instructive to consider the current legislation of the various States and Territories that requires pre-trial disclosure by an accused. For example, the *Criminal Procedure Act 1986* (NSW) states that the purpose of its Division dealing with pre-trial disclosure case management is:

> to enable the court, on a case by case basis to impose pre-trial disclosure requirements on both the prosecution and defence in order to reduce delays in complex criminal trials.[12]

10.21 The court may order pre-trial disclosure on its own initiative or on the application of any party, but may only do so if it is satisfied that the accused person will be legally represented.[13] It also has the power to limit pre-trial disclosure to any

---

9 *R v Lappas and Dowling* [2001] ACTSC 115. See Appendix 4.

10 This was an argument advanced by the Royal Commission on Criminal Justice as cited in the NSW Law Reform Commission, *Discussion Paper 41—The Right to Silence*, <www.lawlink.nsw.gov.au/lrc.nsf/pages/dp41toc>.

11 Center for National Security Studies, *Consultation*, Washington DC, 31 October 2003.

12 *Criminal Procedure Act 1986* (NSW), s 134. The court may require pre-trial disclosure only if it is satisfied that it will be a complex criminal trial, taking into account the estimated duration of the trial, the nature of the evidence to be adduced and the legal issues likely to arise at trial: *Criminal Procedure Act 1986* (NSW), s 136(2).

13 *Criminal Procedure Act 1986* (NSW), s 136(3) and (4).

specified aspect of the proceedings.[14] The pre-trial disclosure regime requires the prosecution to give the accused notice of its case, the accused to give the prosecution notice of the defence response to the prosecution case, and the prosecution to give the defence the prosecution's response to the defence response.[15] The defence response to the prosecution case is required to address a number of matters, including:

> (a) notice as to whether the accused person proposes to adduce evidence at the trial of any of the following contentions:
>
> (i) insanity,
> (ii) self-defence,
> (iii) provocation,
> (iv) accident,
> (v) duress,
> (vi) claim of right,
> (vii) automatism,
> (viii) intoxication,
>
> (b) if any expert witnesses are proposed to be called at the trial by the accused person, copies of any reports by them proposed to be relied upon by the accused person,
>
> (c) the names and addresses of any character witnesses who are proposed to be called at the trial by the accused person (but only if the prosecution has given an undertaking that any such witnesses will not be interviewed before the trial by police officers or the prosecuting authority in connection with the proceedings without the leave of the court),
>
> (d) the accused person's response to the particulars raised in the notice of the case for the prosecution [as provided for by the Act].[16]

10.22 The Act sets out various sanctions for non-compliance with these requirements; for example, the court may refuse to admit evidence sought to be adduced at trial by a party where that evidence was not disclosed to the other party in accordance with these requirements.[17] These pre-trial disclosure requirements do not affect any immunity that applies at law to the disclosure of information, including public interest immunity.[18]

10.23 NSW legislation also contains a power to reduce the sentence for an offence in light of the degree of the accused's pre-trial disclosure. The relevant provisions state that:

---

14 Ibid, s 136(5).
15 Ibid, s 137.
16 Ibid, s 139(1). Among the matters which an accused person's response to the particulars is to contain is whether the accused proposes to dispute the accuracy or admissibility of any proposed documentary evidence, exhibit or other proposed evidence disclosed by the prosecution, and whether the accused intends to dispute any expert evidence relied upon by the prosecution and which evidence is disputed: see *Criminal Procedure Act 1986* (NSW), s 139(2).
17 See *Criminal Procedure Act 1986* (NSW), s 148.
18 Ibid, s 149(6).

> (1) A court may impose a lesser penalty than it would otherwise impose on an offender who was tried on indictment, having regard to the degree to which the defence has made pre-trial disclosures for the purposes of the trial.
>
> (2) A lesser penalty that is imposed under this section in relation to an offence must not be unreasonably disproportionate to the nature and circumstances of the offence.[19]

10.24 Such a power could be included in any proposal to introduce pre-trial disclosure requirements for accused persons in relation to classified or security sensitive information as a means of offsetting some disadvantage caused to them as a result of these provisions.

10.25 The *Crimes (Criminal Trials) Act 1999* (Vic) also imposes pre-trial disclosure obligations on an accused. Under it, an accused must, not less than 14 days before the trial, serve on the prosecution and file in court a defence response to the summary of the prosecution opening and a defence response to the prosecution's notice of pre-trial admissions:[20]

> (2) The defence response to the summary of the prosecution opening must identify the acts, facts, matters and circumstances with which issue is taken and the basis on which issue is taken.
>
> (3) The defence response to the notice of pre-trial admissions must indicate what evidence, as set out in the notice of pre-trial admission, is agreed to be admitted without further proof and what evidence is in issue, and if issue is taken, the basis on which issue is taken.[21]

10.26 The accused is also required to give pre-trial disclosure of the statement of any expert witness he or she intends to call at trial. The expert statement must:

> (a) contain the name and address of the witness;
>
> (b) describe the qualifications of the witness to give evidence as an expert;
>
> (c) set out the substance of the evidence it is proposed to adduce from the witness as an expert, including the opinion of the witness and the acts, facts, matters and circumstances on which the opinion is formed.[22]

10.27 The Victorian Act specifically provides that, apart from the identity of an expert witness, the accused does not have an obligation to provide pre-trial disclosure of any defence witness; nor does the accused have to disclose whether he or she will give evidence.[23]

---

19 *Crimes (Sentencing Procedure) Act 1999* (NSW), s 22A.
20 *Crimes (Criminal Trials) Act 1999* (Vic), s 7(1).
21 Ibid, s 7(2) and (3).
22 Ibid, s 9.
23 Ibid, s 7(4). Section 17 makes it clear that an accused's obligations to disclose the names of witnesses (other than the accused) that he or she intends to call does not arise until the close of the prosecution case.

10.28 The *Criminal Code* (WA) imposes upon an accused person committed for trial the obligation to file and serve on the prosecution:

> (a) a copy of every statement, report or deposition, obtained by the accused person, of any person who may be able to give relevant expert evidence at the trial;
>
> (b) notice of the name and, if known, the address of any person from whom no statement, report or deposition has been obtained but who the accused person thinks may be able to give relevant expert evidence at the trial and a description of the relevant expert evidence concerned;
>
> (c) notice of any factual elements of the offence which the accused may contend cannot be proved;
>
> (d) notice of any objection by the accused person to—
>
> (i) any document that the prosecution proposes to adduce at the trial*;* or
>
> (ii) any evidence disclosed in the statement or deposition of a witness whom the prosecution proposes to call at the trial,
>
> and the grounds for that objection*;* and
>
> (e) notice of any evidence tending to show that the accused person was not present when the offence is alleged to have been committed or an act or omission material to that offence is alleged to have occurred, including—
>
> (i) details of the nature of the evidence*;* and
>
> (ii) details of the name and address of each person whom the accused person proposes to call to give the evidence, or other information sufficient to enable each such person to be located.[24]

10.29 The court has the power to order that any requirement under (a) to (d) above be dispensed with if, on an application by the accused, the court is satisfied that there is a good reason for doing so and that no miscarriage of justice will result. A power of this nature could sensibly be added as part of any proposed regime to introduce pre-trial disclosure requirements for accused persons in relation to classified or security sensitive information in order to ensure that courts can deal with such matters on a case-by-case basis and retain the flexibility to depart from prescribed procedures where it is considered necessary.

10.30 The *Criminal Code Act* (NT) prevents the accused, without leave of the court, from relying on alibi evidence where pre-trial disclosure was not made of that evidence:

> An accused person shall not upon his trial on indictment, without the leave of the court, adduce evidence of an alibi unless, before the expiration of the prescribed

24 *Criminal Code* (WA), s 611C(1). This provision was inserted by *Criminal Law (Procedure) Amendment Act 2002* (WA), s 17.

> period,[25] he gives to the Director of Public Prosecutions written notice of particulars of the alibi and unless the notice contains the name and address of any person whom he claims can support the alibi or, if such name or address is not known to him at the time he gave the notice—
>
> (a) he gives in the notice all information in his possession that may be of material assistance in locating that person; and
>
> (b) the court is satisfied that before giving that notice he had made all reasonable attempts to obtain that name and address and that thereafter he continued to make all reasonable attempts to obtain and to inform the Director of Public Prosecutions of that name and address.[26]

10.31 Defence disclosure requirements for alibi evidence also exist in other jurisdictions, including New South Wales, Tasmania, South Australia, the Australian Capital Territory and Queensland.[27]

Civil proceedings

10.32 In BP 8, the ALRC asked whether Australia needed 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.[28]

10.33 In civil cases, interlocutory processes such as discovery of documents, interrogatories, the issue of subpoenas, and the serving of witness statements and affidavits by all parties to the proceedings will normally raise concerns involving any classified or security sensitive information at an early stage of the proceedings, so that those issues can be dealt with by the court before the final hearing. This would be especially applicable where the relevant government agency is party to, or is otherwise aware of, the proceedings.

10.34 Furthermore, the parties to a civil matter have much greater flexibility to tailor the court's procedures to meet their concerns in relation to the confidentiality of any information that emerges, whether or not it involves classified or security sensitive information, and to settle or otherwise resolve the matter using alternative dispute resolution techniques. These options are not available to the prosecution in a criminal proceeding. Whilst the prosecution in a criminal proceeding may be faced with the choice of disclosing classified information or having to dismiss charges, the government in civil proceedings involving classified information, may have the option, for example, of settling for a lower monetary amount.

---

25 'Prescribed period' is defined as 'the period of 14 days after the date of the committal for trial of the accused person': *Criminal Code Act* (NT), s 331(6).

26 Ibid, s 331(1).

27 See *Criminal Procedure Act 1986* (NSW), s 150, *Criminal Code Act 1924* (Tas), s 368A; *Crimes Act 1900* (ACT), s 288; *Criminal Law Consolidation Act 1935* (SA), s 285C; and *Criminal Code Act 1899* (Qld), s 590A.

28 Australian Law Reform Commission, *Protecting Classified and Security Sensitive Information*, BP 8 (2003), Q 49.

10.35 The courts themselves also have greater flexibility to adjust their procedures in civil proceedings, and the legitimate public interest in open justice arises less starkly in purely private civil matters.

10.36 Nonetheless, certain features of the pre-hearing mechanism proposed by the ALRC would assist in the determination of civil proceedings involving classified or sensitive national security information. In many ways, the ALRC's Proposals may do little more than specify some aspects of powers that civil (and criminal) courts already have. There is nevertheless some value in having these powers enunciated clearly; at the very least, it provides a list of options for the parties and the courts to consider, and reinforces the idea that a careful evaluation of the real need for secrecy combined with some imagination could well allow the parties or the court to fashion a solution in each case that maximises the material that is properly used in the proceedings while still protecting it from dangerous public disclosure. In this way, the proposals attempt to move all participants away from the idea that the public interests in full disclosure and in proper confidentiality are necessarily completely opposed, and that the only solution must necessarily favour one at the expense of the other.

Consultations and submissions

10.37 The Law Council of Australia submitted that it was not opposed to some procedure for determining the admissibility of classified or sensitive information to be used in open court, and noted that existing procedures in most jurisdictions could be used for this purpose.[29] For example, s 391A of the *Crimes Act 1958* (Vic) allows the judge, prior to empanelling a jury, to 'hear and determine any question with respect to the trial of the accused person which the Court considers necessary to ensure that the trial will be conducted fairly and expeditiously'.[30] Such a hearing could encompass issues arising from the anticipated use of classified or security sensitive information. The wording of s 391A seems to suggest that this pre-trial hearing would take place immediately before the jury is empanelled, although it appears to the ALRC that this hearing might be more usefully conducted at an earlier stage of the proceedings.

---

29 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

30 See also *Supreme Court (Criminal Procedure) Rules 1998* (Vic), r 4.09, which provides for a pre-trial conference, and r 4.10, which provides that at any time after a pre-trial conference, the DPP or the accused, or the Criminal Trial Listing Directorate may apply to the Chief Justice for a pre-trial hearing to be conducted by the Court. At a pre-trial hearing the judge may give such directions with respect to the preparation for trial and conduct of the trial as the judge thinks proper having regard to all the circumstances (r 4.10(6)). The pre-trial hearing is to be heard in court and the accused must be present unless the Judge otherwise determines (r 4.10(7) and (8)). *Supreme Court Rules 1970* (NSW), Pt 75, r 11 sets out the pre-trial procedures that must be completed before the trial of a case commences. Part 75, r 11(4) provides that the judge may on his or her own motion or on the application of a party, 'make orders and give directions for the just and efficient disposal of the proceedings'. Such directions could presumably encompass issues arising from the anticipated use of classified or security sensitive information. See also *Criminal Procedure Rules 2000* (WA), Pt 8, r 41, which provides for pre-trial hearings, and *Criminal Code Act 1899* (Qld), s 592A which provides for pre-trial directions and rulings in relation to the conduct of the trial.

10.38 The adoption in Australian legislation of provisions based on or similar to CIPA received some support[31]—for example, in relation to the setting out of express provisions permitting the court to allow unclassified information to be substituted for classified information.[32]

10.39 The Law Council was not convinced that a major overhaul of existing mechanisms for the protection of security sensitive information was warranted, although it stated:

> The Council believes there is a case for exploring the introduction of specialised procedures for dealing with sensitive security information in pre-trial hearings. There is a need for efficient interlocutory processes designed to streamline rather than impede the administration of justice in trials or administrative hearings involving security sensitive information.[33]

10.40 Neither was the Law Council convinced that legislation like CIPA provided a desirable model for reform in Australia.

> First, the scope of CIPA is limited to defence evidence and the problem of dealing adequately with relevant evidence of a classified nature in the hands of the prosecution remains; second, … CIPA may result in the dismissal of the indictment where the defence is ordered not to disclose the information, in which case the grey-mail has succeeded, and third CIPA has generated considerable controversy in the case law as to its scope and purpose.[34]

10.41 The Australian Federal Police submitted that there should be 'processes to apply for exemption from disclosure of unused prosecution material which is remote from the case before a court or tribunal or where this would not substantially compromise the defence case.'[35]

Commission's preliminary views

10.42 The ALRC agrees with the Law Council that any pre-trial mechanism to deal with classified and security sensitive information should sensibly address the issues arising from any classified or security sensitive information proposed to be led or withheld (as the case may be) by either the prosecution or the defence. This would also accommodate the AFP's submission concerning applications for exemption from disclosure by the prosecution, which would be normally dealt with prior to trial. The ALRC anticipates that in some respects the changes that its proposed regime will introduce are greater in appearance than substance. Many courts already have considerable

---

31 Commonwealth Director of Public Prosecutions, *Consultation*, Sydney, 12 November 2003; Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.

32 J Renwick, *Consultation*, Sydney, 9 September 2003.

33 Law Council of Australia, *Submission CSSI 11*, 12 September 2003.

34 Ibid. In support of its latter proposition, the Law Council cited the 7–5 decision of the United States Court of Appeal for the 4th Circuit in *United States v Moussaoui* (2003) US App LEXIS 14073, where it was held that a discovery order granting access to an enemy combatant detained overseas was not appealable under *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 7.

35 Australian Federal Police, *Submission CSSI 13*, 18 September 2003. In this regard see Proposal 10–16.

flexibility to manage their own procedures and to that extent the new regime may simply serve to re-state in one consolidated form powers that already exist but are either tacit, found in the common law, expressed in statute or court rules, or in combinations of these. The fact that these powers are consolidated into a single procedural structure would of itself assist courts and parties to understand their options. The *Lappas* proceedings highlighted the fact that, not least because there have been so few such cases in Australian courts, there was no clear outline of procedures that should or could have been adopted, and that the current statutory statement of state interest immunity[36] was inflexible and led to an undesirable outcome.

10.43 It should be noted that CIPA is not limited to defence evidence. It also covers the discovery of classified information by the US Government and the form in which the discovery of classified documents by it is to take place.[37] In any event, the model proposed by the ALRC is intended to cover all parties in any proceedings in which classified or sensitive national security information is used or likely to emerge.

10.44 The ALRC is not convinced that the threat of greymail is sufficient reason not to set up a specific regime such as it proposes.[38] That threat already exists. Although it is true that CIPA may result in the dismissal of an indictment,[39] so does the current doctrine of state or public interest immunity. If the prosecution wishes to withhold classified or security sensitive information from presentation in court, then, as the *Lappas* case demonstrates, that course of action may lead to the indictment being dismissed in order to preserve an accused's right to a fair trial and to prevent an abuse of process.[40] One advantage of pre-trial disclosure procedures is that they force an early determination of the issues relating to the admissibility and use of classified or security sensitive information so that, if a dismissal or stay of the indictment is likely, it is ordered sooner rather than later, saving resources and time. In any event, a defendant's proposal to lead classified or sensitive national security information in his or her defence will not always be based on a desire to present the prosecution with a greymail threat. In many cases, a defendant may need to present that evidence in order to run his or her defence properly. For example, in prosecutions for unauthorised disclosure of security sensitive information, whenever the content, quality or effect of the information is an issue, it will most likely be an element of the defence, in which case the defendant will need to disclose that information as part of his or her defence, as well as lead evidence relating to its quality or effect. As stated by the US Assistant Attorney General Criminal Division before the Senate Judiciary Committee:

---

36 See *Evidence Act 1995* (Cth), s 130 and 134.

37 See discussion on CIPA in Ch 8.

38 Greymail is discussed in Ch 7 at [7.4] and in Ch 8 at [8.6]–[8.7], [8.55] and [8.128].

39 Although there are exceptions to the dismissal of the indictment when the court determines that the interests of justice would not be served by such a dismissal. These alternatives include 'dismissing specified counts of the indictment or information'; 'finding against the United States on any issue as to which the excluded information relates'; or 'striking or precluding all or part of the testimony of a witness': *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(e)(2).

40 *R v Lappas and Dowling* [2001] ACTSC 115. *Lappas* is discussed in Appendix 4.

> It would be a mistake, however, to view the 'graymail' problem as limited to instances of unscrupulous or questionable conduct by defendants since wholly proper defense attempts to obtain or disclose classified information may present the government with the same 'disclose or dismiss' dilemma.[41]

10.45 The ALRC has been told that CIPA has been reasonably well received in the United States, that it generally works well, and has been fairly successful in getting matters to trial, such as the Iran-Contra case.[42] CIPA forces the prosecution to make certain decisions in relation to its case relatively early, before investing a lot of government resources. Depending on the nature of the matter, the parties need to be prepared to spend considerable time in pre-trial processes.[43] However, the ALRC has been told that CIPA is not always intuitively easy to use and could have been drafted to articulate more clearly the process to be followed[44] and define the material that it covers,[45] which appears in some of its provisions to be limited to writings, recordings and photographs.[46]

10.46 The assignment of court security officers or case managers is specifically provided for in the Guidelines prepared by the Chief Justice of the United States under CIPA.[47] The function of these officers is to assist the court on technical matters, and their use was viewed favourably by various US intelligence agencies.[48] This was also true with regard to the use of specialised courts fitted out for the purpose of hearing matters involving classified and security sensitive information, including the set up of secured classified information facilities at the courthouse.[49] The ALRC understands that in the *Lappas* case an officer of the Australian Federal Police was assigned to assist the Court in connection with the security arrangements that had to be made in relation to the classified and security sensitive material used. As the case was in many

---

41 *Senate Report No 96–823*, United States Congressional and Administrative News, 4294, 4296–4297.

42 United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003; Center for National Security Studies, *Consultation*, Washington DC, 31 October 2003; Federal Bureau of Investigation, *Consultation*, Washington DC, 30 October 2003; Central Intelligence Agency, *Consultation*, Virginia, 24 October 2003. The Center for National Security Studies was involved in the drafting of CIPA with the US intelligence community.

43 Central Intelligence Agency, *Consultation*, Virginia, 24 October 2003. There may be thousands of sensitive documents involved in a case where decisions have to be made in relation to substitution, redaction or summaries, which is why such cases can take so long, up to two or three years in some cases. In addition, the process under CIPA is iterative—the prosecution takes their proposals in relation to disclosure of documents to the judge and, if the judge rejects it because it is unfair to the defendant, the prosecution must try again to satisfy the judge with a different approach to the disclosure of the documents: United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003.

44 Federal Bureau of Investigation, *Consultation*, Washington DC, 30 October 2003.

45 Center for National Security Studies, *Consultation*, Washington DC, 31 October 2003.

46 See *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 8 which is set out in Ch 8 at [8.33].

47 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, [2].

48 The FBI and the Department of Justice have provided court security officers to the court. See discussion on court security officers in Ch 8 at [8.71]–[8.75].

49 United States Attorney's Office—Terrorism and National Security Unit, *Consultation*, Washington DC, 30 October 2003.

ways unique in Australian legal history, it is quite understandable that neither that officer nor the Court nor the participants in the proceedings had any real or direct experience of such cases; nor were there any manuals, guidelines or precedents on which they could rely.

10.47 In 1984, Justice Hope, presiding over the Royal Commission on Australia's Security and Intelligence Agencies, stated that CIPA:

> facilitates the making of informed judgments about the extent to which it might be necessary for classified information to be disclosed in the course, for example, of a prosecution for espionage. I suggest that consideration be given to the need for legislation in Australia to assist the Commonwealth in coping with problems of that kind should they arise.[50]

10.48 The ALRC is not aware of any subsequent move to implement Justice Hope's recommendation.

10.49 The ALRC considers that there is a compelling case for the introduction of a pre-trial mechanism, modelled loosely on CIPA, dealing specifically with the use, relevance, disclosure and admissibility of classified and security sensitive information. However, whereas CIPA is confined to criminal prosecutions, the ALRC considers that its proposed pre-hearing mechanism should also be applied to civil proceedings that may involve the use of classified and sensitive national security information. The mechanism should deal with both the pre-trial disclosure of material in criminal proceedings and discovery, subpoenas, interrogatories and witness statements in civil proceedings, as well as the use of all such material at trial or any final hearing. The use of this material before and during trial are somewhat separate issues as parties will not necessarily seek to admit into evidence every document disclosed or discovered by them before trial, and classified or sensitive national security information may emerge during the trial itself from a third party witness, for example.

10.50 As noted in Chapter 8, the Commonwealth Director of Public Prosecutions' Statement on Prosecution Disclosure appears to be based on the premise that the options available to the prosecution, and indeed to the investigating agency, in relation to disclosure are either full disclosure of sensitive material to the defence or the making of a public interest immunity claim to prevent disclosure. Applications for court-approved alternatives to full disclosure, such as the substitution of unclassified information for classified information, are not raised. This reflects the inflexibility of the current public interest immunity process. Accordingly, there appears to be merit in having express processes to deal with, among other things, the issue of prosecution disclosure to the defence and having a mechanism which sets out the express powers of the court in relation to orders in lieu of full disclosure.

---

50 The Hon Mr Justice Robert Marsden Hope CMG, *Royal Commission on Australia's Security and Intelligence Agencies: General Report* (1984), [4.21].

What material would be covered?

10.51 The new regime should cover all material that is likely to emerge in a case where public or unrestrained disclosure would prejudice Australia's defence or security. Given the definitions of various categories of information described in Chapter 2, the new regime should cover the following classes of classified and sensitive national security information:

- classified national security information;
- security sensitive information (ie, classifiable national security information that has not yet been classified);[51] and
- other national security information which might, if disclosed, prejudice Australia's defence or security.

10.52 The ALRC uses the expression 'sensitive national security information' to cover material in the second and third categories.

10.53 The inclusion of information in the first two categories is self-evident. The third category has been added to ensure that information that warrants some form of protection is not excluded from the regime simply because of a technical, definitional issue. The ALRC anticipates that there would be very few such cases. However, it would be a matter of evidence in every case whether the information in question is of a sort that attracts the new regime. In the case of marked classified information, that would be very easy to prove. However, the ALRC's intention in the new regime is that mere labelling of material is not of itself conclusive—although in many cases no doubt highly persuasive. It is consistent with this approach that inappropriately classified or marked material would not necessarily get the protection of the regime and that unmarked but sensitive material could—it would be a matter of proof in each case.

10.54 The ALRC proposes that the onus of establishing that any material triggers the provisions of the new regime would fall on the party seeking to invoke those provisions, on the balance of probabilities, though the court itself should also have the power to act on its own motion.

10.55 Classified and sensitive national security information may be contained in documents or in oral evidence, or both. The new regime should cover both.

10.56 The new regime should also cover information that may emerge as evidence or likely evidence at or before any final trial or hearing of the matter, or that might emerge in any pre-trial process, such as discovery of documents, interrogatories and the issue of subpoenas, even though it may not be tendered at the trial or final hearing.

---

51 See the discussion of the expression 'security sensitive information' in Ch 2 at [2.16]–[2.19].

10.57 The new regime should cover the whole range of documents that could be subject to the rules of disclosure and discovery. In this regard, existing definitions of 'document' in Australian legislation could be adopted. For example, Federal Court Rules, Order 1 Rule 4 provides that:

> **document** includes any record of information which is a document within the definition contained in the Dictionary in the Evidence Act 1995 and any other material data or information stored or recorded by mechanical or electronic means.

10.58 'Document' is defined in Part 1 of the Dictionary contained in the *Evidence Act 1995* (Cth) as 'any record of information', and includes:

> (a) anything on which there is writing; or
>
> (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
>
> (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
>
> (d) a map, plan, drawing or photograph.[52]

10.59 There is much to be said for keeping the definition of 'document' in the proposed regime the same as that in the *Evidence Act* since both statutes relate to the handling of evidence in court. The definition from that Act quoted in the previous paragraph appears to be comprehensive enough to cover classified and security sensitive information, but the ALRC would be interested to learn whether classified or sensitive national security information could be conveyed or recorded on some medium not covered.

Basic proposal: a National Security Information Procedures Act

10.60 The ALRC proposes that the Australian Parliament enact a new piece of legislation—a National Security Information Procedures Act—to deal specifically and solely with the protection of classified and sensitive national security information in court, tribunal and similar proceedings. The procedure to be promulgated by that Act should adhere to the statements of principle set out in the following paragraphs and summarised in the boxed paragraphs at the end of this Chapter: see Proposal 10–1 and following.

Scope of the new Act

10.61 The Act should cover the use of all classified national security information and sensitive national security information, whether contained in a document (as defined in the *Evidence Act*) or in oral evidence.

---

52 *Evidence Act 1995* (Cth), cl 8, Part 2 of the Dictionary provides that a reference in the Act to document includes a reference to (a) any part of the document; (b) any copy, reproduction or duplicate of the document or of any part of the document; or (c) any part of such a copy, reproduction or duplicate.

10.62 'Sensitive national security information' should be defined to include:

(a) 'national security information' as defined in the Commonwealth *Protective Security Manual* that should have been classified but has not been classified; and

(b) any other national security information which might, if disclosed, prejudice Australia's defence or security.

10.63 The new Act should cover all stages of proceedings in all Australian courts and tribunals.

Early notification

10.64 The scheme should require each party to any proceeding to inform the court and the other parties as soon as it becomes aware that any information covered by the new Act is likely to emerge at any stage in the case. This may well be apparent at the outset; however, it might only become clear as the case develops. It could conceivably not arise until the final hearing or trial, or even conceivably at sentencing, although the ALRC anticipates that this would be unlikely in a well prepared case. Once the court has been notified, it must convene a directions hearing to review the issues that arise in relation to the handling of the sensitive material. The court may also convene such a directions hearing of its own motion.

10.65 If the government agency concerned with the sensitive material is not a party, or if the case is not a prosecution by the Commonwealth Director of Public Prosecutions (CDPP), the court must notify, or must direct a party to notify, the Australian Attorney-General to ensure that the appropriate government agency is aware of the possible disclosure of classified or sensitive national security information. The Attorney-General would have the right to intervene in the proceedings, but only on these issues. The obligation to notify would not arise in a prosecution by the CDPP on the basis that the CDPP is instructed by or is in contact with the Attorney-General's Department or the relevant government agency, and would be alert to these issues once they arise.

List of classified or sensitive national information

10.66 Subject to any orders given by the court, the proposed regime would require all parties in a proceedings to file and serve lists of all classified or sensitive national security information that they reasonably anticipate will be used in the proceedings, either in their own case or in rebuttal to the case of any other party. The lists should also include any such material that they anticipate may come from third parties—for example, in response to subpoenas or in giving evidence at the trial or final hearing. The court may make such directions as it thinks fit in relation to the specificity with which classified or sensitive national security information is to be described in these lists, the people to whom these lists are to be given, the use that may be made of the information contained in them, and the degree of protection that must be given to them.

The court's powers generally

10.67 Once the court is aware that classified or sensitive national security information may be used in the case, the new Act would give it the power to make orders to govern the handling of that information from time to time over the course of the proceedings. The court may make those orders of its own motion or on the motion of any of the parties or the Attorney-General intervening. The regime gives an indicative range of the orders that a court and the parties may consider as options. This list is not intended to be exhaustive or exclusive; its purpose is to indicate the breadth of options specifically authorised by the Act without shutting out any other options that the court may find appropriate and useful.

10.68 The options include a variety of orders for the substitution of the classified or security sensitive information with unclassified or less sensitive material, alternative evidence from unclassified sources, statements of fact (whether agreed by the parties or not), statements of admission, summaries of the sensitive material and so on. In each instance, the use of this material is subject to the court's approval.[53]

Closed courts

10.69 The court may decide to hear some or all of the proceedings in the absence of the public. Subject to certain safeguards set out in detail below, in civil cases and tribunal proceedings, where required or authorised by statute, the court or tribunal may decide to hear a portion of the proceedings in the absence of one or more of the parties. The absent party should, however, be at all times represented by a lawyer, whether his or her own, or other counsel appointed by the court to protect that person's interests.[54] The court may decide that certain material may be shown only to individuals with an appropriate security clearance. Subject to certain safeguards, the court may decide that certain material may not be made available to the public or particular individuals (including parties), diverging from the court rules that would otherwise apply. In all these situations, the power to determine how the proceedings will be run would rest with the court. All parties and the Attorney-General intervening would have the right to seek orders governing the use and protection of the classified and sensitive national security information and would have the right to be heard on these questions before the determinations are made.

10.70 If the court sees fit, it may give leave to representatives of the media or other public interest groups to be heard, but that would be in line with whatever powers the court may have in that respect. The ALRC does not propose that there be any specific requirement that the media be notified of any application or order to close a court.

---

53 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003. It has also been stated that an important feature of the CIPA procedures is that the court controls the redaction of the classified information by the executive: J Renwick, *Consultation*, Sydney, 9 September 2003.

54 The questions of closed courts and secret evidence are discussed in more detail below starting at [10.102] and [10.120] respectively.

Objectives of the scheme

10.71 A principal aim of the ALRC's proposed regime is to flush out issues relating to the use of classified and sensitive national security information as early in the proceedings as circumstances permit. This would help all participants understand the likely progress of the matter. It would allow the Government and other parties concerned with the way in which certain material is to be handled to approach the court for the orders they seek, if necessary returning to the court with alternative proposals in the light of the development of the evidence and the court's previous rulings. For example, the prosecution might apply on a number of occasions with different approaches to the use of especially sensitive material. Although the court should be slow to restrict these applications, all participants would be aware that the need to progress the matter and the demands of proper case management militate against excessively repeated attempts to introduce problematic evidence. The possibility of making a number of applications seeking to have classified or sensitive national security information introduced into a proceeding but nonetheless granted an appropriate level of protection gives the Government much greater opportunity to consider its options concerning the use of the material in question. The Government also receives the benefit of a greater opportunity than it has now to revise its case to take into account the limitations on the use of the sensitive information imposed on it by the nature of that material and the court's rulings. For example, it can amend the details of the charges—such as the dates of, or parties to, an alleged conspiracy—so that sensitive material becomes irrelevant (and therefore removed from the case entirely) and the case can then proceed on the basis of less contentious evidence.

10.72 The court's ultimate concern is that the case proceed as far as it can with all admissible evidence before it with the critical proviso that all parties are given a fair hearing or a fair trial, and that any departures from the usual standards of judicial process are limited to those strictly necessary to protect the national interest. To this end, the court must retain the power to dismiss, stay, discontinue or strike out all or part of any party's case where that is required in the interests of justice.

10.73 It also follows that the court should retain the power to make whatever costs or other similar orders are appropriate to reflect the consequences of any other orders it makes under this regime.

Particular options

10.74 Either on the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may make orders for the further conduct of the proceedings and the use of classified or sensitive national security information, including but not limited to:

(a) Determinations of the relevance and admissibility of any classified or sensitive national security information;

(b) The form in which any classified or sensitive national security information may be tendered to the court as evidence or otherwise used in the proceedings. Such orders may involve:

(i) the redaction, editing or obscuring of any part of a document containing or adverting to classified or sensitive national security information;

(ii) replacing the classified or sensitive national security information with summaries, extracts or transcriptions of the evidence that a party seeks to use, or by a statement of facts, whether agreed by the parties or not;

(iii) replacing the classified or sensitive national security information with evidence to similar effect obtained through unclassified means or sources;

(iv) concealing the identity of any witness or person identified in, or whose identity might be inferred from, classified or sensitive national security information or from its use in court (including oral evidence);

(v) the use of written questions and answers during otherwise oral evidence;

(vi) closed-circuit television, computer monitors, headsets and other technical means in court by which the contents of classified or sensitive national security information may be obscured from the public or other particular people present in court;

(vii) restrictions on the people to whom any classified or sensitive national security information may be given or to whom access to that information may be given;[55]

(viii) restrictions on the extent to which any person who has access to any classified and sensitive national security information may use it; and

(ix) restrictions on the extent to which any person who has access to any classified and sensitive national security information (including any juror) may reproduce or repeat that information.

10.75 The court should retain the flexibility to deal with evidence (most probably oral testimony) revealing classified or sensitive national security information previously found by the court to be inadmissible or which is raised unexpectedly at the hearing, perhaps during cross-examination or by a third party. Where there is concern that testimony will reveal classified or sensitive national security information, a party might be required to provide the court with a proffer of the witness's response to the question

55 For example, the court may order that such material only be given to people with a security clearance at a specified level.

or line of enquiry, and requiring any other party questioning the witness to provide the court with a proffer of the nature of the information that it seeks to elicit.

10.76 On the application of any party or of the Attorney-General of Australia intervening, or on its own motion, the court may order that the whole or any part of a proceedings be heard in the absence of:

(a) any one or more specified people; or

(b) the public.

Undertakings and security clearance

10.77 The court may require undertakings from any party in the proceedings, their legal representatives, or both, on such terms as the court sees fit, about the confidentiality and limits on use to be attached to any classified or sensitive national security information. These undertakings may be in addition to, or in substitution for, any other requirement made by the court or the Act, or sought by any party to the proceedings or the Attorney-General of Australia (including but not limited to any requirement that a party or its legal representatives obtain any security clearance).

Public interest immunity

10.78 Nothing in the new Act should affect the right of a party or the Government to make an application under s 130 of the *Evidence Act 1995* (Cth) (state interest immunity). Section 130 and related provisions apply to material other than classified and security sensitive information and should remain in place to cater for those situations. Those provisions might become redundant to the extent that they relate to classified and security sensitive information although they still have a function in relation to other forms of sensitive information.

Ancillary matters

10.79 If a party fails to comply with the requirements of the Act or the orders of the court the court may make such orders as its Rules permit including, but not limited to, orders preventing a party tendering or otherwise seeking to use certain material or from calling or examining certain witnesses, and orders staying, discontinuing, dismissing or striking out that party's case in part or whole.

10.80 A party may be excused from non-compliance with the requirements of the Act or the orders of the court if:

(a) the party has good reason;

(b) there is no miscarriage of justice; and

(c) there is no disclosure of classified or sensitive national security information that is not otherwise permitted or authorised by law.

10.81 The court should have the power to reduce sentences to take into account pre-trial disclosure by the accused.

10.82 In criminal matters, the court may order that the prosecution be excused in part or whole from any obligation that it would otherwise have been under to disclose information to an accused person, or that any such obligation be varied.

10.83 So far as possible, the evidence in support of any application for any order under the new Act should be in open court and, when on affidavit, not sealed.

Statements of reasons and transcripts

10.84 There appears to be some merit in the US approach requiring the issue of specific findings of fact justifying the closure of criminal proceedings.[56] Such an approach could legitimately be extended to criminal and civil proceedings in Australia. This would appear to sit comfortably with the general principle that a court should only order closure of a court as a last resort.[57] The ALRC considers that whenever there is any restriction on the basic principles of open courts and the right to a public hearing, the court's judgment on those issues should be set out in a statement of reasons. This would mean that whenever a court makes an order for an in-camera hearing or a suppression order, such as an order restricting publication of proceedings or restricting access to documents on the court file, to protect classified or security sensitive information, it should provide reasons for so doing. The act of providing reasons on those issues serves as a salutary discipline in ensuring that the court has properly considered the necessity of making such an order, and that the order made is a proportionate response to the issues igniting the need for the order. Further, as noted in Chapter 7 the giving of reasons is a normal incident of the judicial process[58] and should be adopted in relation to the making of any order under the new Act.

10.85 Accordingly, the ALRC proposes that full written reasons for any order or finding made under the proposed Act should be prepared by the court. The court may then determine to what extent (if at all) those reasons should be sealed, published and distributed to the parties or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect the classified or sensitive national security information used in proceedings, the court should ensure that any party whose rights are adversely affected by the order receives a copy of the reasons that allows it to pursue any avenue of appeal that may be open.

10.86 A full transcript should be prepared of any proceedings heard in the absence of any one or more specified people, the public, any one or more parties, or the legal representatives of any one or more parties. The court may then determine to what extent (if at all) that transcript should be sealed, published and distributed to the parties

---

56 See discussion in Ch 8 at [8.233]–[8.235].
57 See discussion in Ch 8 at [8.207]–[8.209].
58 See Ch 7 at [7.102].

or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect the classified or sensitive national security information used in proceedings, the court should ensure that all parties receive a copy of the transcript that allows them to pursue any avenue of appeal that may be open.

10.87 On the application of any party to the proceedings or of the Attorney-General of Australia intervening or any other person, or on its motion, the court may order that any sealed written reasons for any order or any sealed transcript of any proceedings (or any part of them) may be unsealed, published or distributed on a wider basis than the court had previously ordered.

10.88 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may review any order it makes in relation to the use of classified or sensitive national security information in proceedings. For example, the court may order the disclosure of material that it had previously ordered could be withheld or introduced in another fashion, in the light of subsequent developments in the proceedings or elsewhere which alter the requirements of justice in the case or reduce the sensitivity of the material in question.

10.89 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its motion, the court may order that any specified person (including but not limited to any party's legal representatives, court staff, court reporters, expert witnesses or other participant in the proceedings) seek a security clearance to a specified level appropriate to the classified or sensitive national security information used in the proceedings. The court may also make orders with respect to who must bear the costs of processing any such clearance. Alternatively, the court may order that specified material not be disclosed to any person who does not hold a security clearance at a specified level.

10.90 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may order that the whole or any part of a proceeding be stayed, discontinued, dismissed or struck out if the protection of any classified or sensitive national security information requires that it not be fully disclosed to the court or to a party with the result that any party's rights and ability to fairly and freely present its case and to test the case of, and evidence tendered by, any other party is unfairly diminished.

10.91 The court may make such orders as it sees fit in relation to costs and the adjournment of the whole or any part of the proceedings as a result of any requirement of the new Act, order of the court, conduct of the parties or otherwise in relation to the use of classified or sensitive national security information in any proceedings.

10.92 The court may impose such conditions as it sees fit (including the stay, discontinuance, dismissal or striking out of any proceedings in part or whole) on any order that it might make under the new Act.

10.93 A court must permit an appeal (if one is sought) from any order requiring any disclosure of any classified or sensitive national security information to be fully determined before any such disclosure is made. Where necessary, a court should grant any leave that might be required by any party in order to pursue any such appeal.

10.94 Any other appeals from any order relating to the use of classified or sensitive national security information in proceedings should follow the normal procedures applicable in the court seized of the matter. However, an appeal from any order restricting the access by any party or its legal representatives to any material which is otherwise used in the proceedings and to which other parties have greater access should be fully determined before the primary proceedings proceed to final hearing or trial.

Ministerial statements and certificates

10.95 Other than in the most exceptional circumstances, the law should not permit a statement of any minister, member of the government, statutory office-holder or other government entity to determine the use (or restrictions on the use) of any classified or sensitive national security information in any court proceedings where that determination would, under these principles, have otherwise been made by the court. In many cases, of course, any statement by the Attorney-General or other minister or appropriate statutory office-holder will be given significant weight by the court.

10.96 However, the Attorney-General of Australia or any other person authorised by statute may issue a certificate stipulating that certain classified or sensitive national security information is not to be disclosed to any, or any specified, person in the course of legal proceedings. The court must then determine whether, in the light of that certificate, the proceedings should be stayed, discontinued, dismissed or struck out in part or whole. The ALRC expects that no such certificate would be issued until all other measures under the Act have been tested. The purpose of the Act is to maximise the possibility that all relevant evidence is before the court in a way that is fair to all parties and to maximise the public access to the proceedings. However, if the material in question is simply so sensitive that it cannot be disclosed at all, the final power to withhold it rests with the Attorney-General. In turn, the final power to determine the manner in which the case will proceed rests with the court, and the ultimate result could be that the action is brought to an end. This could mean, in an extreme example, that the issue of such a certificate by the Government that has the effect of thwarting in whole or part its opponent's case could lead a court to staying the *Government's* case in whole or part if the result would otherwise be that an apparently legitimate claim is negated by the unreviewable decision of the party (that is, the Government) against which it is made.

10.97 Ministerial certificates about classified and security sensitive information involved in court or tribunal proceedings should be as expansive as circumstances permit to allow the court or tribunal to make an informed decision on the appropriate handling of classified and security sensitive information. Where appropriate, such certificates should be accompanied by statements or affidavits from subsidiary decision

makers or other officers briefing the Minister, explaining the decision-making process and, if necessary, why the information that might otherwise seem uncontroversial does in fact have national security implications.

10.98 As a matter of principle, the classification status of a document may carry significant weight on its own, but should never be determinative on the issue of closure of a court.

10.99 As is always the case, the court must at all times be alert to ensure that no party's ability to present its case fairly and freely and test the case and evidence presented by each other party is unfairly diminished.

10.100 Courts should amend their own Rules to the extent necessary to implement the scheme contained in the proposed new Act.

Technical assistance

10.101 The relevant Australian Government department or agency—probably the Protective Security Coordination Centre—should train and assign one or more officers to the federal and other courts, on a permanent basis, to assist the courts in ensuring the protection of any classified or sensitive national security information that is used in proceedings. Such officers would be answerable to the courts to which they are assigned and would advise the courts on (apart from other matters) technical aspects of the physical storage and handling of classified or sensitive national security information. However, they would not independently purport to advise the court about the need to protect any material that is not the subject of any court order or ministerial or other certificate.

Courts closed to the public

10.102 The ALRC's preliminary view in relation to the closure of courts at any stage of the proceedings is that the court should retain the ultimate discretion to determine whether or not to hold a hearing or part of a hearing in camera or to make a suppression order, following a consideration of evidence led by the party seeking such an order and any party opposing it. The court may invite the media to make submissions but the ALRC is not inclined to propose that there be any requirement to do so or to notify them of the application to close the court.[59] Statements of ministers—whether in the form of affidavits or otherwise—supporting an application for a hearing in camera or a suppression order, should not be determinative, although in many cases significant weight would be attached to any such statement. As far as possible, the evidence in support of an application to hold an in-camera hearing or to make a suppression order should be given in open court and be open to testing by the parties whose interests might be affected by the making of the order.

---

59 See the discussion at [10.110] below.

10.103 By way of contrast, in the United States under CIPA, hearings to determine the use, relevance and admissibility of classified information must be held in camera if the Attorney General certifies to the court that a public proceeding may result in the disclosure of classified information.[60] Similarly, hearings of motions by the US Government for an alternative order to full disclosure of classified information must be held in camera at the request of the Attorney General.[61] Both these provisions require the court to hold these interlocutory hearings in camera on the Attorney General's certification or request; there is no room for judicial discretion in this regard. The ALRC considers that it would be preferable to allow the court to determine whether or not to hold a pre-trial hearing in camera, following a consideration of evidence led by the party seeking such an order. Such an approach would also be less likely to offend Chapter III of the *Australian Constitution*.[62]

10.104 The Attorney-General's Department has submitted that:

> [W]here the court retains the discretion to close or open the proceedings where security classified information is at issue, security classified information is at potential risk of disclosure.[63]

10.105 In one sense, that is inevitably true. However, the ALRC's preliminary view is that this is no basis to compel the closure of *all* court proceedings where security classified information is involved. This would go against the principle, discussed in Chapter 8,[64] that closure of courts should be a last resort and that, wherever possible, protective measures short of closure should be adopted. It therefore ignores the possibility that in many cases other mechanisms, such as redaction of information or the handing up of documents without reading them out to the court, may be an effective, and indeed a more proportionate, response in dealing with such information.[65]

10.106 The ALRC proposal contemplates that a court will (as it does now) assess the level of possible damage caused by the release of classified or security sensitive information and weigh this against the public interest in having the matter proceed in open court. In this regard, the proposed new Act should include a provision, modelled loosely on s 35(3) of the *Administrative Appeals Tribunal Act* 1975 (Cth),[66] to provide that, in considering an application to close the court or issue a suppression order, the court shall take as the basis of its consideration the principle that it is desirable that hearings be held in public, and that evidence given before the court and the contents of documents admitted into evidence should be made available to the public and to the

---

60 See *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(a).
61 See Ibid, s 6(2)(c).
62 See the discussion in Ch 9 under the heading 'Courts closed to a party'.
63 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
64 See Ch 8 at [8.207]–[8.209].
65 See Ch 7 at [7.89] on proportionality and Ch 8 at [8.251] in relation to HREOC's submission that any safeguard imposed upon the use of closed hearings should reflect the requirement of proportionality.
66 See Ch 7 at [7.13].

parties.[67] The court should also pay due regard to any reason given to it why the court should be closed or why the publication or disclosure of the evidence should be prohibited or restricted. This would accommodate the submission of the Australian Press Council that courts should be required to give regard to the public interest in maintaining open hearings prior to ordering a closed court.[68]

10.107 In relation to the Australian Press Council submission that s 93.2 of the *Criminal Code* be amended to provide specifically that the court give regard to the principles of open justice prior to ordering a closed hearing,[69] the proposed new Act would render s 93.2 obsolete. Both that section and s 85B of the *Crimes Act 1914* (Cth) should then be repealed.

10.108 Any legislative provision requiring the closure of *all* proceedings where classified or sensitive national security information is involved runs the risk of being invalid.[70] In *John Fairfax Publications Pty Ltd v Attorney-General*, the NSW Supreme Court considered s 101A(7) and 101(8)(a) of the *Supreme Court Act 1970* (NSW), which respectively required an appeal by the Attorney-General on questions of law from an acquittal for criminal contempt to be heard in camera and submissions made on that appeal not to be published. These provisions were held to be invalid. Spigelman CJ stated:

> [W]hen the parliament prescribed in subs (7) that the whole of any proceedings must be in camera, it went well beyond what was required in order to serve the objective of the legislation. Similarly when, in subs (8)(a), parliament prohibited the publication of any report of any submission made under subs (1) of that section, it also went beyond what was required in order to serve that objective.
>
> In each case the prohibition attaches to every aspect of the hearing of the application, whether protective of the person entitled to anonymity, or not. The substance of the issues to be determined will generally be of broader significance and will not involve or require revelation of the identity of the acquitted contemnor.
>
> In my opinion, in these two respects the parliament went too far in the sense that it intruded into the freedom of communication guaranteed by the Constitution in a manner not reasonably appropriate and adapted to achieving the legitimate objective of protecting persons who have been acquitted of criminal contempt.[71]

10.109 As discussed in Chapter 7, the principle of open justice is a fundamental aspect of the rule of law, especially in relation to the right to a fair trial, and ensures public confidence in the administration of justice. Accordingly, the principles of open

---

67 However, depending on the nature of the documents, the leave of the court may be required to obtain access in accordance with established court rules

68 See Ch 8 at [8.249].

69 See Ch 8 at [8.248]–[8.249].

70 See also discussion on Chapter III considerations in Ch 9 under the heading 'Courts closed to a party' where it is noted that openness is an ingredient of the judicial process and that any provision which would require the court to act in a manner inconsistent with the judicial process is at risk of infringing Chapter III.

71 *John Fairfax Publications Pty Ltd v Attorney-General* (2000) 181 ALR 694, [127]–[129].

justice and fair trials must be borne in mind when considering orders made by the court for in camera hearings and the making of orders restricting publication of proceedings and restricting access to documents on the court file in order to protect classified and security sensitive information.

10.110 At this stage, the ALRC is not minded to make a proposal based on the US approach that, before closing criminal proceedings, the court must give notice of its intention to do so to ensure that the press and the public be given a meaningful opportunity to be heard on the question of their exclusion. The logistics of implementing such an approach are not clear. It could be difficult to determine precisely whom the court would have to give notice. For example, who would constitute the press for the purposes of such a provision? Would the court have to give notice to every major national and regional newspaper as well as radio and television stations and news-oriented websites or it would it have to issue a press release? It would be difficult to justify requiring courts to give notice to the media in cases involving intended closure of proceedings to protect classified or security sensitive information, but not in other cases where closure is intended (for example, for the protection of a witness's safety). However, to require the courts to give notice to the media in every instance where the court intends to close proceedings, or part of proceedings, for whatever reason, and to make it mandatory to give the media an opportunity to be heard in all such cases would introduce delay into the hearings of proceedings.

10.111 Further, there is no reason why the parties involved in the proceedings cannot notify the media themselves in relation to any proposed closure of court proceedings. In circumstances where media organisations are unable to make representations against closure, it is always open to them after the proceedings have been conducted to apply for release of the transcript. In other words, the possibility exists for closed hearings to become public after the event. In any event, it is open to the courts to give the media an opportunity to be heard on any orders restricting their access to the proceedings or the documents filed in them. This happened in the *Lappas* proceedings.[72]

10.112 One of the essential safeguards of an in-camera hearing is that records of that hearing in the form of a full and complete transcript should be kept and preserved to facilitate any review or appeal procedure. Accordingly, at this stage, the ALRC does not adopt the submission of the Law Society of New South Wales to the extent that it encompasses the possibility that a court could order that no transcript be made of proceedings closed to the public.[73] The ALRC proposes that the court determine on a case-by-case basis who should have access to the transcript, how it should be stored, and the duration, extent and review mechanisms of any conditions which may be imposed on access. It should also be left to the court to determine on a case-by-case basis whether an edited version of the transcript, which has references to classified and security sensitive information deleted, should be prepared and whether the media and

72 See Appendix 4, [17].
73 See Ch 8 at [8.255]–[8.256].

public should be allowed access to it, and the conditions of such access. At this stage, the ALRC is not convinced about the necessity for a third version of the transcript to be possibly prepared to assist lawyers in the preparation of like cases.[74] In all events, however, the starting point should remain that a full record of all proceedings be made, kept, made available to the parties and published. The court then has the power to determine whether and to what extent exceptional circumstances exist that would warrant any departure from this.

10.113 The Australian Press Council has submitted that copies of all evidence tendered in cases conducted either in camera or in secret be retained.[75] The ALRC notes that upon completion of proceedings or after the expiry of the period in which an appeal can be instituted, it is usual for the court to return exhibits to the parties.[76] Persons seeking access to such exhibits can seek them directly from the parties involved. At present, the ALRC is not convinced that it is necessary for the court to retain copies of all exhibits tendered in an in-camera hearing beyond the period that it would normally retain them.

10.114 The Australian Press Council also submitted that edited or summarised versions of documents containing classified or security sensitive information should be provided to the public where access to the full document is restricted.[77] The legislative scheme proposed by the ALRC—see in particular Proposal 10–10—allows the court to make a number of orders in relation to the use of classified and sensitive national security information, including the form in which such information may be tendered to the court as evidence or otherwise used in the proceedings. If, for example, the court ordered that a redacted or summarised version of a document containing classified or security sensitive information be tendered in evidence or otherwise used in the proceedings, that would be the form of the document in respect of which the public could seek access, either with or without the leave of the court, depending on the particular court rules governing the proceedings.[78] This proposal makes specific reference to the court's power to determine whether access may be granted to certain evidence, which would encompass a power to determine whether accessible evidence is in an edited or redacted form.

10.115 The Australian Press Council submitted that it may be appropriate to formulate voluntary principles to guide journalists who are considering the publication of security sensitive information.[79] Where court proceedings have been the source of that information, it is difficult to conceive what the scope of such voluntary principles would be. If the court has allowed access to proceedings involving classified or security sensitive information and not made any orders restricting or prohibiting the reporting of the

---

74 See J Söderblom, *Submission CSSI 5*, 25 August 2003, noted in Ch 8 at [8.258].
75 See Ch 8 at [8.259] and Ch 9 at [9.106].
76 For example, see *Supreme Court Rules 1970* (NSW), Pt 75 r 31 and *Supreme Court (Criminal Procedure) Rules 1998* (Vic), r 2.18.
77 See Ch 8 at [8.249].
78 See discussion in Ch 7 at [7.22]–[7.25].
79 See Ch 8 at [8.262].

proceedings, the media would not be restricted in their publication of the information, subject to their complying with any relevant laws such as the laws governing defamation and contempt. Where, however, the court has made an order restricting or prohibiting the reporting of the proceedings, the media are bound by that order.

10.116 There may, however, be some scope for the application of such voluntary principles in circumstances where the media has gained access to security sensitive information from sources other than court proceedings. In this regard, the ALRC is interested in hearing further from the Australian Press Council and other media organisations as to the benefits of formulating voluntary principles to guide journalists in considering the publication of sensitive material, or amending the journalists' code of conduct to deal specifically with the use of classified and security sensitive information. The ALRC notes that, as the code of conduct is voluntary, there may be issues about its unenforceability. Of course, any such guidelines or codes of conduct should be publicised widely to ensure that courts, prosecutors, defence lawyers, other court participants and the general public are aware of their contents.

Tribunals closed to the public

10.117 The same principles that apply to court proceedings should generally apply to tribunal proceedings and royal commissions.[80] There is, of course, a difference to the extent that legislation requires a tribunal to hold closed hearings in certain specified circumstances. However, the same principles in relation to keeping of transcripts of closed proceedings and the requirement to give reasons for a decision to close a tribunal hearing or a discretionary decision to issue a suppression order should apply.

10.118 The Australian Press Council submitted that royal commissions should be required to allow the media to make submissions as to whether or not proceedings should be heard in camera.[81] The ALRC is not presently inclined to make any recommendation requiring courts or tribunals to notify the media about any application or order to close proceedings, and sees no reason to create an exception for royal commissions. The commissioners may choose to invite the media to make submissions, and media present (through their legal advisers) will often seek to do so.[82]

10.119 As noted in Chapter 8, the view has been expressed that, while the risk of accidental disclosure is high in court, it is higher in the AAT in particular because more sensitive material is used in that forum. The ALRC is not aware whether tribunals that hold hearings involving classified or security sensitive information have in place internal guidelines or procedures in relation to the handling and storage of such material, and whether tribunal staff receive training in the implementation of these guidelines. If

---

80 It has been noted that royal commissions, unlike courts and tribunals, do not determine rights. However, people's reputations and other significant interests may be harmed by the public discussion of untested material or by public speculation on undisclosed evidence.

81 See Ch 8 at [8.250] and Australian Press Council, *Submission CSSI 17*, 5 December 2003.

82 See also [10.110].

not, these guidelines should be developed and put into effect by the tribunals concerned.

Secret evidence

10.120 The use for any purpose of evidence that is not freely available to all parties—especially the party against whom it is led or to the person whose interests may be adversely affected by reliance upon it (such as a visa applicant)—should be countenanced only in the most exceptional circumstances. In this section, the ALRC uses the term 'secret evidence' to mean evidence that is not disclosed to a party or a person whose interests are affected by an official decision based on it. In some cases, the affected person is aware that such evidence exists but cannot obtain access to it; in other cases, the affected person does not even know that it exists or that it is being used against him or her, in which case the hearings themselves are also secret.

10.121 As a matter of principle, the leading of secret evidence against an accused, for the purpose of protecting classified or security sensitive information in a criminal prosecution, should not be allowed. To sanction such a process would be in breach of the protections provided for in Article 14 of the International Covenant on Civil and Political Rights for an accused to be tried in his or her presence and to have the opportunity to examine, or have examined any adverse witnesses. Where such evidence is central to the indictment, to sanction such a process would breach basic principles of a fair trial, and could constitute an abuse of process.

10.122 The leading of secret evidence against a party in civil proceedings should not generally be allowed except in exceptional circumstances, and subject to certain safeguards.[83] Secret evidence must always be considered as a last resort, after the court has determined that the alternative methods available to it to protect the information are not adequate in the circumstances. However, a distinction can be made between the use of secret evidence in different types of civil proceedings. For example, it is harder to justify the use of secret evidence where a party is denied access to evidence led against it in primary proceedings as opposed to judicial review proceedings. In the former type of proceedings, the court has greater powers to ensure that parties are given access to all the evidence.

10.123 One type of civil proceeding is judicial review of administrative decisions based on evidence withheld from a party, an example of which is *Mohammed El Amer v Minister for Immigration, Local Government and Ethnic Affairs*.[84] In proceedings of this nature where an applicant is seeking access to evidence withheld by the administrative decision-maker, the court may affirm the decision of the original administrative decision-maker not to disclose the information, or set aside the decision and remit the matter back to the original decision-maker for reconsideration according to law. The court is unable to substitute its own decision and, for example, give the applicant

83 These safeguards are discussed at [10.138] below.
84 See discussion in Ch 9 at [9.64].

access to the withheld material.[85] The safeguard is that the court reviews for itself whether the information is of such a sensitive nature to warrant being withheld from the party affected. It is not clear from *El Amer* whether the original administrative decision-maker considered alternatives to complete non-disclosure. For example, it is not clear whether consideration was given to disclosing to the applicant a redacted version of the ASIO security assessment, or an unclassified summary of its contents.

10.124 Secret evidence—whether in the form of a confidential affidavit or oral evidence in the absence of a party—used to determine a claim for public interest immunity (or other preliminary question) rather than any substantive issue may be less objectionable. In any event, the fact that the claim is being made and the general basis for it should made known to the other party. Not every hearing of a public interest immunity claim will call for the leading of secret evidence; whether it does is a matter for determination by the court.

10.125 Similarly, there is less objection in principle to having a mechanism in place, which may, in part, involve the leading of secret evidence to determine whether the prosecution's obligation to disclose a particular document can be dispensed with, or dealt with in an alternative manner.[86] Dispensation of the disclosure requirement is akin to a successful public interest immunity claim in that it will usually mean that the document in question will not be adduced in evidence and will not be relied upon by the Court against the accused.[87] There is no reason in principle why such applications should not be conducted in a similar manner to a public interest immunity claim.[88] Such a procedure should be conducted with notice to the accused and the basis of the prosecution's application for dispensation should also be made known to the accused. In this regard, the ALRC is of the preliminary view that the *Justices Act 1902* (WA)[89] should not be used as a model as it allows the dispensation application to be determined without notice to the accused—hence the accused may not even be made aware of the existence of the application, let alone its basis. Furthermore, the provisions in that Act are not comprehensive in relation to the disclosure or admission of classified or sensitive national security information. For example, the Act is silent about both the consequences of non-disclosure and alternatives to non-disclosure.

---

85 See *Minister for Immigration and Ethnic Affairs v Guo* (1997) 191 CLR 559, 578–579, 598–600, where it is stated (at 598–599) that, 'Whereas on appeal a court will often enjoy the power and responsibility of substituting its decision for that under appeal, judicial review is designed, fundamentally, to uphold the lawfulness, fairness and reasonableness (rationality) of the process under review. It is thus ordinarily an adjunct to, and not a substitution for, the decision of the relevant administrator.'

86 Or indeed, whether a party's obligation to discover classified or security sensitive material in a civil proceedings can be dispensed with or dealt with in an alternative manner.

87 The court, should, of course, have regard to the issue of whether the document sought to be exempt from disclosure would assist the defendant in his or her defence.

88 As stated in Ch 9 at **[**9.10**]** the evidentiary basis of the claim is publicly exposed so far as can be done without revealing the nature or the content of the material for which the immunity is claimed, and the fact that additional confidential evidence has been provided to the judge is not kept secret.

89 See discussion in Ch 9 at [9.11**]**.

10.126 Apart from general principles of fairness, any legislation that would *require* a court to hear classified and security sensitive evidence in the absence of an accused would fall foul of Chapter III of the *Australian Constitution*. It appears that even legislation which would permit the court to do so runs a real risk of infringing Chapter III as it would be authorising a process not in accordance with judicial process.[90] For this reason the ALRC does not propose legislation that would give the courts such a power in order to protect classified and security sensitive information.

10.127 The Attorney-General's Department submitted that the *Migration Legislation Amendment (Protected Information) Act 2003* (Cth)[91] provided a useful precedent for legislation to protect classified and security sensitive information.[92] However, there are some concerns associated with adopting this legislation as a general precedent outside the particular and specialised context for which it was developed. As noted in Chapter 9, this legislation allows the Federal Court and the Federal Magistrates Court in certain circumstances to rely on evidence that is not divulged to the applicant or the applicant's legal representatives. One concern is that the legislation does not provide for any alternative method of disclosure to the applicant of the secret evidence relied upon; nor does it contain other safeguards that are a feature of comparative international legislation. Further, it gives the Minister the ultimate decision whether to release confidential information to the courts in circumstances where the Minister is not required to justify or account for that decision. The Minister does not have a duty even to consider the exercise of his or her power to make a declaration authorising disclosure to the court. In replacing public interest immunity, the legislation has limited the role of the judiciary in providing an independent check on the exercise of executive power.

10.128 A review of international legislation permitting the use of secret evidence, discussed in Chapter 9, shows that a common feature of such schemes is the provision of a summary of the evidence taken in a party's absence to be provided to the party, or the making of rules allowing such a summary to be provided to the absent party. This is the case in respect of certain judicial review hearings under the Canadian *Criminal Code*[93] as well as hearings before a judge under the *Charities Registration (Security Information) Act 2001* (Canada) and the *Immigration and Refugee Protection Act 2001* (Canada). In each case, the judge must provide to the absent party a summary of the information available to the judge without disclosing information that would injure national security or endanger the life of a person, and, in addition, provide the absent party an opportunity to be heard.[94]

10.129 In the UK, the *Anti-Terrorism Crime and Security Act 1981*, the *Terrorism Act 2000*, the *Regulation of Investigatory Powers Act 2000* and the *Special Immigration*

---

90 See discussion in Ch 9 under heading 'Courts closed to a party', particularly at [9.20].
91 This legislation is discussed in Ch 9 at [9.56]–[9.62].
92 Attorney-General's Department, *Submission CSSI 16*, 25 November 2003.
93 [RS 1985, c C-46].
94 See discussion in Ch 9 at [9.35]–[9.38] and [9.75].

Appeals Commission Act 1997[95] all permit or require the relevant Commission or Tribunal to make rules in relation to providing a party with a summary of evidence taken in his or her absence.

10.130 In the US, an alien (ie, a non-citizen) facing deportation proceedings before the US Alien Terrorist Removal Court (ATRC), while not entitled to see classified evidence or be informed as to its sources, is entitled to an unclassified summary of specific evidence that does not pose a risk to national security or to the security of a person.[96] The summary must be sufficient to enable the alien to prepare a defence and the summary is to be approved by the ATRC.[97] The alien is also entitled to be represented by a security-cleared lawyer who can challenge the veracity of the classified evidence in an in-camera proceeding.[98]

10.131 The *Special Immigration Appeals Commission Act 1997* (UK) also has an extra safeguard in providing that a person may be appointed to represent the interests of an appellant in any proceedings from which the appellant and his or her lawyer are excluded. The *Special Immigration Appeals Commission (Procedure Rules) 2003* (UK) provide that the Secretary of State may not rely upon evidence that it objects to disclosing to a party or their lawyer in a proceeding before SIAC unless a special advocate has been appointed to represent the interests of the absent party.[99] None of these safeguards found in international legislation is present in the *Migration Legislation Amendment (Protected Information) Act 2003* (Cth).

10.132 As noted in Chapter 9, one of the criteria under the *Migration Legislation Amendment (Protected Information) Act 2003* to which the Federal Court of Australia and the Federal Magistrates Court must have regard in making a non-disclosure order is the fact that the information was communicated to an authorised migration officer by a gazetted agency on the condition that it be treated as confidential information. There is no requirement that the information be confidential or warrant treatment as such. The Act does not define 'confidential information'. For example, there is no apparent correlation to the definition of 'confidential' in the *Commonwealth Protective Security Manual*, where it is set out to be one of the four national protective security markings.[100] Where the Minister decides to withhold the information from the court, there is no ability to test the nature of the information, including its confidentiality, as the Minister's decision to withhold the information from the court is not subject to review. On its face, this criterion of confidentiality appears to be a relatively low and uncertain benchmark on which to base a non-disclosure order by the court. Of course, there are other criteria to which the court must have regard in making such an order, and the court has the discretion not to make a non-disclosure order.

---

95 See discussion in Ch 9 at [9.47]–[9.49] and [9.71].
96 8 USC (US), s 1534(3)(A) and (3)(B).
97 See Ibid, s 1534(3)(C) and (D).
98 See Ibid, s 1532(e) and s 1534(F).
99 See Ch 9 fn [161].
100 As discussed in Ch 2 at [2.8], the Confidential marking is given to information, the disclosure of which could cause 'damage' to national security.

10.133 The options available to the Federal Court or the Federal Magistrates Court in dealing with the information under the Act are limited. The court will either never have access to the information itself or, where the Minister authorises disclosure to the court, it can make interim or permanent non-disclosure orders on the application of the Minister or refuse to make such non-disclosure orders. It would be desirable for the courts to be able to consider a greater number of options in making an order resulting in the withholding of evidence from an affected party. The principle that secret evidence should only be used as a last resort in the most exceptional matters in order to protect classified or sensitive national security information highlights the desirability for statutory provisions modelled on CIPA, which expressly sets out the powers of a court to make orders in lieu of full disclosure.

10.134 As discussed in Chapter 9, many tribunals already have the power, or are required by statute, to rely on secret evidence. Tribunals are not bound by the same Chapter III considerations that bind federal courts. However, while there may not be the same constitutional issues for tribunals, the issues of principle remain.[101] The ALRC considers that the provisions of the regime under the proposed new Act, including those that relate specifically to the use of secret evidence, should apply equally to courts and tribunals, although legislation may in some exceptional cases authorise divergence from these principles in relation to tribunals.

10.135 As noted in Chapter 7, some minimum procedural protections guaranteed by international law apply exclusively to criminal proceedings. In *Detroit Free Press v John Ashcroft*,[102] 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.

10.136 In light of the serious consequences that flow from deportation and other similar proceedings, the ALRC is of the preliminary view that certain minimum protections should extend to persons facing these types of hearings to militate against the use of

---

101 Advisory Committee members, *Advisory Committee meeting*, 19 September 2003.

102 *Detroit Free Press v Ashcroft* (Unreported, US Court of Appeals for the 6th Circuit, Keith and Daughtrey (Circuit Judges) Carr (District Judge), 26 August 2002), 12.

secret evidence. Similar protections should apply to all persons facing tribunal hearings, whatever their nature, where secret evidence may be adduced or relied upon. In this regard, the ALRC is attracted to HREOC's submission that 'wherever the rights of a defendant are diminished there should be some compensating protection'.[103]

10.137 The ALRC intends that one of the safeguards that should apply to the adducing of secret evidence in tribunal matters is that the normal rules of evidence should apply, to the maximum extent allowed by the legislation establishing the tribunal. The ALRC is mindful that legislation establishing tribunals (and royal commissions) can provide that tribunals are not bound by the rules of evidence.[104] However, as secret evidence already represents a significant erosion of a party's rights, no further departure from the normal rules of evidence should be allowed. This would ensure, for example, that the rules against hearsay evidence would apply to the adducing of any secret evidence. It would also ensure the application of the rules of practice relating to ex parte hearings.

10.138 In summary, the ALRC's preliminary views in relation to the use of secret evidence, to the extent that they are not already covered by the basic proposals under the new Act set out earlier in this chapter, are as follows:

(a) The use of any secret evidence is highly undesirable but, if it is necessary and (in the case of tribunals) authorised or required by statute, then safeguards should be in place;

(b) Ministerial certificates should generally not be determinative of the manner in which any evidence may be used;

(c) Before consenting to any application that evidence be led in secret, the court or tribunal should consider alternative methods of presenting that evidence such as summaries, stipulations and redactions—which are to be approved by the court or tribunal before use;

(d) The affected person should always be represented by a lawyer, even if that lawyer is not one of the person's choosing, but rather a court-appointed lawyer holding any requisite security clearances;

(e) Any tribunal proceedings involving secret evidence should be heard by a judicial member of the tribunal;

(f) There should be an avenue of appeal available to courts on the question whether the secret evidence should be disclosed to the affected person;

---

103 Human Rights and Equal Opportunity Commission, *Submission CSSI 12*, 12 September 2003. See Ch 9 at [9.89],

104 See, for example, *Administrative Appeals Tribunal Act 1975* (Cth), s 33(1)(c).

(g) The affected person should always be notified of the fact that secret evidence is being used against him or her; and

(h) The normal rules of evidence should apply, including those that involve ex parte hearings.

Secret hearings

10.139 The fact that a hearing is taking place should generally not be kept from the party whose rights or interests are being determined or affected by the hearing, whether that hearing is in a court or a tribunal. However, there are some exceptions where notification to the affected person would destroy the whole purpose of the hearing in the first place—notably hearings in relation to applications for search warrants and applications for approval to adopt other investigative tools. In these cases, the hearing is in fact often a judicial check on the use by police or the executive government of invasive methods of investigation that require monitoring in the public interest.

10.140 It should be left to the discretion of the court or tribunal whether there is a need to keep the fact of a hearing secret from the public for a temporary period of time. Permanent suppression from the public of the fact that a hearing has taken place should not be permitted except in extraordinary circumstances.

10.141 In all cases where a hearing is conducted in secret, a transcript or full record of the proceedings, and a written statement of reasons for the court or tribunal's decision, should be made. These would normally be sealed in line with the secrecy attaching to these proceedings. However, such material would become an essential tool in considering the legitimacy of the decision if ever challenged.

A single court?

10.142 The ALRC has considered whether it would be desirable or possible to centralise cases involving classified and sensitive national security information in a single court (or a small number of courts) so that expertise could be collected in one place and the extra resources that would be needed to handle a flow of such cases—should that ever arise—would be minimised.

10.143 For example, the US District Court for the Eastern District of Virginia has specially-built facilities for the storage of classified information.[105] Having a centralised court would assist in the development of specialist expertise in handling cases involving classified and security sensitive information. This would include a pool of judges and lawyers practising in the court with experience in the legal and practical issues surrounding such cases. Court staff could be trained and, where necessary, security cleared. However, it must be remembered that these cases remain extremely rare in Australia and it may be difficult to justify the expenditure of significant resources to

105 Federal Bureau of Investigation, *Consultation*, Washington DC, 30 October 2003.

install facilities that would not be used often. The appointment of technical security officers to the courts hearing matters involving classified and security sensitive information would in some way deal with this issue.[106]

10.144 It would be attractive in some respects to declare that all such cases would be heard in, for example, the Federal Court of Australia or the courts of the Australian Capital Territory (where one imagines that a relatively high proportion of such cases would be heard in any event). However, the *Australian Constitution* provides some obstacles. Section 80 provides that:

> The trial on indictment of any offence against any law of the Commonwealth shall be by jury, **and every such trial shall be held in the State where the offence was committed**, and if the offence was not committed within any State the trial shall be held at such place or places as the Parliament prescribes. [emphasis added]

10.145 Therefore, it appears that the geographical centralisation of these matters would require a constitutional amendment. Even if the Federal Court (or any other federal court) were designated as the principal court for espionage trials or matters involving classified and security sensitive information, it would need to be given criminal jurisdiction. This would not, however, overcome the constitutional requirement that the trial be held in the State (or Territory) in which the offence is alleged to have occurred. The Federal Court would still have to hear matters where they arose. Although the venue might still have to be the State or Territory in which the alleged crime was committed, the fact that the Federal Court is a national court would allow some specialisation. This would simply require the appropriate allocation of judges and other resources (as already happens in other areas of that court's areas of specialised jurisdiction). A more significant problem (and cost) would be the need to expand the Court's expertise in criminal matters.[107]

10.146 Accordingly, despite the logical and practical attractions, the ALRC does not make any proposal in relation to the centralisation of matters involving classified and security sensitive information in any one court or location. However, the ALRC would be interested in hearing further from any interested party on that question.

Summary of Proposals

10.147 The reforms that the ALRC suggests be distilled into a new National Security Information Procedures Act stated in various places in this Chapter can be summarised by the following Proposals.

---

106 See Proposal 10–36.

107 See Australian Law Reform Commission, *The Judicial Power of the Commonwealth*, ALRC 92 (2001).

Proposal 10–1 The Australian Parliament should enact a National Security Information Procedures Act to deal specifically and solely with the protection of classified and sensitive national security information in court, tribunal and similar proceedings. The procedures to be promulgated by that Act should adhere to the statements of principle set out in the following Proposals.

Proposal 10–2 The Act should cover the use of all classified national security information and other sensitive national security information, whether contained in a document (as defined in the *Evidence Act*) or in oral evidence.

Proposal 10–3 For the purposes of the new Act, 'sensitive national security information' should be defined to include:

(a) 'national security information' as defined in the Commonwealth *Protective Security Manual* that should have been classified but has not been classified; and

(b) other national security information which, if disclosed, might prejudice Australia's defence or security.

Proposal 10–4 The new Act should apply to all stages of proceedings in any Australian court in which classified or sensitive national security information arises.

Proposal 10–5 Each party to proceedings should be required to give notice to the court and to all other parties as soon as practicable after it becomes aware that classified or sensitive national security information is reasonably likely to be used in those proceedings—whether during interlocutory steps (such as discovery, interrogatories and witness statements prepared and exchanged by the parties before any final hearing or trial in the proceedings), at any eventual hearing or trial in the proceedings or in any other way.

Proposal 10–6 The court may of its own motion give the parties in any proceedings the notice referred to in Proposal 10–5.

Proposal 10–7 In civil proceedings or criminal proceedings not conducted by the Commonwealth Director of Public Prosecutions, the court must notify, or direct one or more parties in the proceedings to notify, the Attorney-General of Australia that the notice referred to in Proposal 10–5 or Proposal 10–6 has been given. The Attorney-General of Australia has the right to intervene in the proceedings only in relation to all issues concerning the use of classified or sensitive national security information arising in them.

Proposal 10–8 Once the required notice has been given, the court must hold a directions hearing or similar interlocutory process to determine the future conduct of the proceedings in relation to the use of classified and sensitive national security information. The court may hold such hearings as may be necessary from time to time.

Proposal 10–9 Subject to any orders given by the court, all parties in a proceeding shall file and serve lists of all classified or sensitive national security information that they reasonably anticipate will be used in the proceedings, whether in their own case or in rebuttal to the case of any other party. The court may make such directions as it thinks fit in relation to the specificity with which classified or sensitive national security information is to be described in these lists, the people to whom these lists are to be given, the use that may be made of the information and the degree of protection that must be given.

Proposal 10–10 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may make orders for the further conduct of the proceedings and the use of classified or sensitive national security information, including but not limited to:

(a) Determinations of the relevance and admissibility of any classified or sensitive national security information, including any claims for public interest immunity;

(b) The form in which any classified or sensitive national security information may be tendered to the court as evidence or otherwise used in the proceedings. Such orders may involve:

  (i) the redaction, editing or obscuring of any part of a document containing or adverting to classified or sensitive national security information;

  (ii) replacing the classified or sensitive national security information with summaries, extracts or transcriptions of the evidence that a party seeks to use, or by a statement of facts, whether agreed by the parties or not;

  (iii) replacing the classified or sensitive national security information with evidence to similar effect obtained though unclassified means or sources;

(iv) concealing the identity of any witness or person identified in, or whose identity might reasonably be inferred from, classified or sensitive national security information or from its use in court (including oral evidence), and concealing the identity of any person (including jurors) who come into contact with classified or sensitive national security information;

(v) the use of written questions and answers during otherwise oral evidence;

(vi) closed-circuit television, computer monitors, headsets and other technical means in court by which the contents of classified or sensitive national security information may be obscured from the public or other particular people in court;

(vii) restrictions on the people to whom any classified or sensitive national security information may be given or to whom access to that information may be given (which may include limiting access to certain material to people holding security clearances to a specified level);

(viii) restrictions on the extent to which any person who has access to any classified and sensitive national security information may use it; and

(ix) restrictions on the extent to which any person who has access to any classified and sensitive national security information (including any juror) may reproduce or repeat that information.

Proposal 10–11 The court should retain the flexibility to deal with evidence revealing classified or sensitive national security information previously found by the court to be inadmissible or which is raised unexpectedly at the hearing.

Proposal 10–12 Nothing in the proposed new Act should affect the right of a party or the Government to make an application for state interest immunity under s 130 of the *Evidence Act*.

Proposal 10–13 If a party fails to comply with the requirements of the Act or the orders of the court the court may make such orders as its Rules permit including, but not limited to, orders preventing a party tendering or otherwise seeking to use certain material, and from calling or examining certain witnesses, and orders staying, discontinuing, dismissing or striking out that party's case in part or whole.

Proposal 10–14 A party may be excused from non-compliance with the requirements of the Act or the orders of the court if:

(a) the party has good reason;

(b) there is no miscarriage of justice; and

(c) there is no disclosure of classified or sensitive national security information that is not otherwise permitted or authorised by law.

Proposal 10–15 The court should have the power to reduce sentences to take into account the co-operation of the accused with respect to pre-trial disclosure.

Proposal 10–16 In criminal matters, the court may order that the prosecution be excused in part or whole from any obligation that it would otherwise have been under to disclose information to an accused person, or that any such obligation be varied.

Proposal 10–17 On the application of any party or of the Attorney-General of Australia intervening, or on its motion, the court may order that the whole or any part of a proceedings be heard in the absence of:

(a) any one or more specified people; or

(b) the public.

Proposal 10–18 The proposed new Act should include a provision, modelled loosely on s 35(3) of the *Administrative Appeals Tribunal Act 1975* (Cth), to provide that:

(a) in considering an application to close the court to the public or to any party, the court shall take as the basis of its consideration the principle that it is desirable that hearings be held in public and in the presence of all parties;

(b) that evidence given before the court and the contents of documents admitted into evidence should be made available to the public and to the parties, though depending on the nature of the documents the leave of the court may be required to obtain access in accordance with established court rules;

(c) the court should pay due regard to any reason given to it as to why the court should be closed or why the publication or disclosure of the evidence should be prohibited or restricted.

Proposal 10–19 So far as possible, the evidence in support of any application for any order under the new Act should be in open court and, when on affidavit, not sealed.

Proposal 10–20 Written reasons for any order or finding under the new Act should be prepared. The court may then determine to what extent (if at all) those reasons should be sealed, distributed to the public and to the parties or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect classified or sensitive national security information used in proceedings, the court should ensure that any party whose rights are adversely affected by the order receives a copy of the reasons that allows it to pursue any avenue of appeal that may be open to it.

Proposal 10–21 A full transcript of any proceedings heard in the absence of any one or more specified people, the public, any one or more parties, or the legal representatives of any one or more parties should be prepared. The court may determine to what extent (if at all) that transcript should be sealed or distributed to the public and to the parties or their legal representatives. To the greatest extent reasonably possible consistent with the court's determination on the need to protect classified or sensitive national security information used in proceedings, the court should ensure that all parties receive a copy of the transcript that allows them to pursue any avenue of appeal that may be open to them.

Proposal 10–22 On the application of any party to the proceedings or of the Attorney-General of Australia intervening or any other person, or on its motion, the court may order that any sealed written reasons for any order or any sealed transcript of any proceedings (or any part of them) may be unsealed or published on a wider basis than the court had previously ordered.

Proposal 10–23 The court may require undertakings from any party in the proceedings, their legal representatives, or both, on such terms as the court sees fit, as to the confidentiality and limits on use to be attached to any classified or sensitive national security information. These undertakings may be in addition to, or in substitution for, any other requirement made by the court or the proposed new Act, or sought by any party to the proceedings or the Attorney-General of Australia (including but not limited to any requirement that a party or its legal representatives obtain any security clearance).

Proposal 10–24 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its motion, the court may order that any specified person (including but not limited to any party's legal representatives, court staff, court reporters, expert witnesses or other participant in the proceedings) seek a security clearance to a specified level appropriate to the classified or sensitive national security information used in the proceedings. Alternatively, the court may order that specified material not be disclosed to any person who does not hold a security clearance at a specified level. The court may also make orders about who shall bear the costs of any such clearance.

Proposal 10–25 On the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its motion, the court may order that the whole or any part of a proceedings be stayed, discontinued, dismissed or struck out if the protection of any classified or sensitive national security information requires that it not be fully disclosed to the court or to a party with the result that any party's rights and ability to fairly and freely present its case and to test the case of, and evidence tendered by, any other party is unfairly diminished.

Proposal 10–26 The court may make such orders as it sees fit in relation to costs and the adjournment of the whole or any part of the proceedings as a result of any requirement of the proposed new Act, order of the court, conduct of the parties or otherwise in relation to the use of classified or sensitive national security information in any proceedings.

Proposal 10–27 The court may impose such conditions as it sees fit (including the stay, discontinuance, dismissal or striking out of any proceedings in part or whole) on any order that it might make under the proposed new Act.

Proposal 10–28 Either on the application of any party to the proceedings or of the Attorney-General of Australia intervening, or on its own motion, the court may review any order it makes in relation to the use of classified or sensitive national security information in proceedings. For example, the court may order the disclosure of material that it had previously ordered could be withheld or introduced in another fashion in the light of subsequent developments in the proceedings or elsewhere which alter the requirements of justice in the case or reduce the sensitivity of the material in question.

Proposal 10–29 A court must permit an appeal (if one is sought) from any order requiring any disclosure of any classified or sensitive national security information to be fully determined before any such disclosure is made. Where necessary, a court should grant any leave that might be required by any party in order to pursue any such appeal.

Proposal 10–30 Any other appeals from any order relating to the use of classified or sensitive national security information in proceedings should follow the normal procedures applicable in the court seized of the matter. However, an appeal from any order restricting the access by any party or its legal representatives to any material which is otherwise used in the proceedings and to which other parties have greater access should normally be fully determined before the primary proceedings proceed to final hearing or trial.

Proposal 10–31 Except in the most exceptional circumstances, the law should not permit a statement of any minister, member of the government, statutory office-holder or other government entity to determine the use (or restrictions on the use) of any classified or sensitive national security information in any court proceedings where that determination would, under these principles, have otherwise been made by the court. Any statement by the Attorney-General or other minister or appropriate statutory office-holder would, of course, be given significant weight.

Proposal 10–32 The Attorney-General of Australia or any other person authorised by statute may issue a certificate stipulating that certain classified or sensitive national security information is not to be disclosed to any, or any specified, person in proceedings. The court must then determine whether, in the light of that certificate, the proceedings should be stayed, discontinued, dismissed or struck out in part or whole.

Proposal 10–33 Ministerial certificates about classified and security sensitive information involved in court or tribunal proceedings should be as expansive as circumstances permit in order to allow the court or tribunal to make an informed decision on the appropriate handling of classified and security sensitive information. Where appropriate, such certificates should be accompanied by statements or affidavits from subsidiary decision–makers or other officers briefing the Minister, explaining the decision-making process and, if necessary, why the information that might otherwise seem uncontroversial does in fact have national security implications.

Proposal 10–34 The classification status of a document on its own should never determine any matter under the new Act.

Proposal 10–35 Courts and tribunals should amend their own Rules to the extent necessary to implement the practices and procedures in the proposed new Act, including guidelines in relation to the handling and storage of classified and sensitive national security information.

Proposal 10–36 The relevant Australian Government department or agency should train and assign one or more officers to the federal and other courts, on a permanent basis, to assist the courts in ensuring the protection of any classified or sensitive national security information that is used in proceedings. Such officers would be answerable to the courts to which they assigned and would advise the courts on, apart from other matters, technical aspects of the physical storage and handling of classified or sensitive national security information. However, they would not independently purport to advise the court about the need to protect any material that is not the subject of any court order or ministerial or other certificate.

Proposal 10–37 Section 93.2 of the *Criminal Code Act 1995* (Cth) and s 85B of the *Crimes Act 1914* (Cth) should be repealed.

Proposal 10–38 An accused person and his or her legal representatives should have access to all evidence tendered against him or her.

Proposal 10–39 The taking of evidence involving classified or security sensitive information in civil proceedings before a court or tribunal in the absence of a party whose interests are affected, or the withholding of such evidence received by a court or tribunal from a party in circumstances where the court or tribunal intends to rely on that evidence, should not be permitted where that evidence represents the only or the major piece of evidence against the absent party.

Proposal 10–40 The taking of evidence involving classified or security sensitive information in civil proceedings before a court or tribunal in the absence of a party whose interests are affected, or the withholding of such evidence received by a court or tribunal from a party in circumstances where the court or tribunal intends to rely on that evidence, should not be permitted except in the most extraordinary circumstances, and then only subject to the following safeguards:

(a) Ministerial certificates should generally not be determinative of the way in which any evidence may be used;

(b) Before consenting to any application that evidence be led in secret, the court or tribunal should consider alternative methods of presenting that evidence such as summaries, stipulations and redactions—which are to be approved by the court or tribunal before use;

(c) The affected person should always be represented by a lawyer, even if that lawyer is not of the person's choosing but a court-appointed lawyer holding any requisite security clearances;

(d) Any tribunal proceedings involving secret evidence should be heard by a judicial member of the tribunal;

(e) There should be an avenue of appeal available to courts on any question of whether the secret evidence should be disclosed to the affected person;

(f) The affected person should always be notified of the fact that secret evidence is being used against him or her;

(g) The normal rules of evidence should apply, including those that involve ex parte hearings; and

(h) A complete record of the whole of the proceedings, including a written statement of reasons for any decision or order made, should be prepared and kept by the court or tribunal. The court or tribunal may determine on a case-by-case basis what (if any) access to the record of proceedings may be permitted.

Proposal 10–41 The fact that a hearing is taking place should never be kept from the party whose rights or interests are being determined or affected by the hearing, whether that hearing is in a court or a tribunal. However, this Proposal is *not* intended to cover hearings in relation to applications for search warrants and applications for approval to adopt other investigative tools.

Proposal 10–42 It should be left to the discretion of the court or tribunal whether there is a need to keep the fact of a hearing secret from the public for a temporary period of time. Permanent suppression from the public of the fact that a hearing has taken place should only be allowed in exceptional circumstances.

Appendix 1. List of Submissions

Name	*Submission no*	*Date*
Administrative Appeals Tribunal	CSSI 3	28 May 2003
Attorney-General's Department	CSSI 16	25 November 2003
Australian Crime Commission	CSSI 15	13 October 2003
Australian Federal Police	CSSI 13	18 September 2003
Australian Press Council	CSSI 17	5 December 2003
Mr Robert Cock QC, Director of Public Prosecutions for Western Australia	CSSI 6	28 August 2003; 16 September 2003
Mr Harry Evans, Clerk of the Senate	CSSI 4	25 August 2003
Human Rights and Equal Opportunity Commission	CSSI 12	12 September 2003
Law Council of Australia	CSSI 11	12 September 2003
Law Society of New South Wales	CSSI 9	28 August 2003
Merit Protection Commissioner	CSSI 10	29 August 2003
National Legal Aid	CSSI 8	3 September 2003
NSW Bar Association	CSSI 2	11 April 2003
NSW Police	CSSI 7	29 August 2003
Mr Jason Söderblom	CSSI 5	25 August 2003
Victoria Legal Aid	CSSI 14	26 September 2003
The Victorian Bar	CSSI 1	8 April 2003

Appendix 2. Abbreviations and Acronyms

The various entities listed below are Australian unless otherwise stated.

AAT	Administrative Appeals Tribunal
AAT Act	*Administrative Appeals Tribunal Act 1975* (Cth)
ACC	Australian Crime Commission
ACSI	Australian Communications Electronic Security Instruction
ACT	Australian Capital Territory
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
BP 8	Background Paper 8, *Protecting Classified and Security Sensitive Information*
CDPP	Commonwealth Director of Public Prosecutions
CIA	Central Intelligence Agency (USA)
CIPA	*Classified Information Procedures Act* (USA)
Crimes Act	*Crimes Act 1914* (Cth)
CSE	Communications Security Establishment (Canada)
CSIS	Canadian Security and Intelligence Service
CSIS Act	*Canadian Security and Intelligence Service Act 1984*
CTC	Competitive tendering and contracting
DDIS	Directorate of Defence Intelligence and Security (NZ)
DIA	Defence Intelligence Agency (USA)
DIGO	Defence Imagery and Geospatial Organisation
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs

DIO	Defence Intelligence Organisation
DIS	Defence Intelligence Staff (UK)
DP	This Discussion Paper
DPP	Director of Public Prosecutions (usually referring to the Commonwealth DPP)
DSD	Defence Signals Directorate
ECHR	European Court of Human Rights
EO 13292	*Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information* (USA)
Evidence Act	*Evidence Act 1995* (Cth)
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)
GCHQ	Government Communications Headquarters (UK)
GCSB	Government Communications Security Bureau (NZ)
HREOC	Human Rights and Equal Opportunity Commission
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*]
ISC	Intelligence and Security Committee (UK)
ISCAP	Interagency Security Classification Appeals Panel (USA)
ISOO	Information Security Oversight Office (USA)
LECD	Law Enforcement Coordination Division [of the Attorney-General's Department]
MI5	British Security Service
MI6	Secret Intelligence Service (UK)
MRT	Migration Review Tribunal
NAA	National Archives of Australia
NARA	National Archives and Records Administration (USA)
NCTC	National Counter-Terrorism Committee
NLA	National Legal Aid
NPPs	National Privacy Principles [under the *Privacy Act 1988* (Cth)]
NRO	National Reconnaissance Office (USA)
NSA	National Security Agency (USA)
NTAC	National Threat Assessment Centre
NZSIS	New Zealand Security Intelligence Service
ONA	Office of National Assessments
PCO	Privy Council Office (Canada)

PII	Public interest immunity
POAC	Proscribed Organisations Appeal Commission
Privacy Act	*Privacy Act 1988* (Cth)
PSCC	Protective Security Coordination Centre
PSM	*Commonwealth Protective Security Manual*
RCMP	Royal Canadian Mounted Police
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
RSAA	Refugee Status Appeals Authority (NZ)
SIAC	Special Immigration Appeals Commission (UK)
SIRC	Security Intelligence Review Committee (Canada)
SIS	Secret Intelligence Service (UK)
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)
UNHCR	United Nations High Commissioner for Refugees
USC	United States Code
VCAT	Victorian Civil and Administrative Tribunal
VLA	Victoria Legal Aid
WA Guidelines	Statement of Prosecution Policy and Guidelines for the Office of Public Prosecutions of Western Australia

Appendix 3. Extracts from Statute

The following extracts include most of the principal provisions referred to in the text of this Paper found in Australian and overseas statutes and in key international instruments. Provisions referred to in passing only or otherwise adequately set out in the text and footnotes are not included in this Appendix.

Contents

Australian Constitution

Chapter III—The Judicature

Section 71

The judicial power of the Commonwealth shall be vested in a Federal Supreme Court, to be called the High Court of Australia, and in such other courts as the Parliament creates, and in such other courts as it invests with federal jurisdiction. …

Section 75

In all matters—

(i) Arising under any treaty:

(ii) Affecting consuls or other representatives of other countries:

(iii) In which the Commonwealth, or a person suing or being sued on behalf of the Commonwealth, is a party:

(iv) Between States, or between residents of different States, or between a State and a resident of another State:

(v) In which a writ of Mandamus or prohibition or an injunction is sought against an officer of the Commonwealth:

the High Court shall have original jurisdiction.

Section 80

The trial on indictment of any offence against any law of the Commonwealth shall be by jury, and every such trial shall be held in the State where the offence was committed, and if the offence was not committed within any State the trial shall be held at such place or places as the Parliament prescribes.

Australian Security Intelligence Organisation Act 1979 (Cth)

Section 18—Communication of intelligence etc.

(1) The communication of intelligence on behalf of the Organisation shall be made only by the Director-General or by a person acting within the limits of authority conferred on the person by the Director-General.

(2) If a person makes a communication of any information or matter that has come to the knowledge or into the possession of the person by reason of his or her being, or having been, an officer or employee of the Organisation or his or her having entered into any contract, agreement or arrangement with the Organisation, being information or matter that was acquired or prepared by or on behalf of the Organisation in connection with its functions or relates to the performance by the Organisation of its functions, other than a communication made:

(a) to the Director-General or an officer or employee of the Organisation:

(i) by an officer or employee of the Organisation—in the course of the duties of the officer or employee; or

(ii) by a person who has entered into any such contract, agreement or arrangement—in accordance with the contract, agreement or arrangement;

(b) by a person acting within the limits of authority conferred on the person by the Director-General; or

(c) with the approval of the Director-General or of an officer of the Organisation having the authority of the Director-General to give such an approval;

the first-mentioned person is guilty of an offence.

Penalty: Imprisonment for 2 years.

(3) Notwithstanding paragraph 17(1)(b), the Director-General or a person authorised for the purpose by the Director-General may, in accordance with the following paragraphs, communicate information that has come into the possession of the Organisation in the course of performing its functions under section 17:

(a) where the information relates, or appears to relate, to the commission, or intended commission, of an indictable offence against the law of the Commonwealth or of a State or Territory—the information may be communicated to an officer of the Police Force of a State or Territory, to a member or special member of the Australian Federal Police or to the Chief Executive Officer of the Australian Crime Commission or a member of the staff of the ACC; or

(b) where the information has come into the possession of the Organisation outside Australia or concerns matters outside Australia and the Director-General or the person so authorised is satisfied that the national interest requires the communication—the information may be communicated to:

(i) a Minister; or

(ii) a Department; or

(iii) an intelligence or security agency; or

(iv) an officer of a Police Force of a State or Territory; or

(v) a member or special member of the Australian Federal Police; or

(vi) the Chief Executive Officer of the Australian Crime Commission or a member of the staff of the ACC.

(5) A prosecution for an offence against subsection (2) shall be instituted only by or with the consent of the Attorney-General.

Crimes Act 1914 (Cth)

Part IC—Investigation of Commonwealth offences

Division 3—Obligations of investigating officials

Section 23V—Tape recording of confessions and admissions

(1) If a person who is being questioned as a suspect (whether under arrest or not) makes a confession or admission to an investigating official, the confession or admission is inadmissible as evidence against the person in proceedings for any Commonwealth offence unless:

(a) if the confession or admission was made in circumstances where it was reasonably practicable to tape record the confession or admission—the questioning of the person and anything said by the person during that questioning was tape recorded; or

(b) in any other case:

(i) when questioning the person, or as soon as practicable afterwards, a record in writing was made, either in English or in another language used by the person during questioning, of the things said by or to the person during questioning; and

(ii) as soon as practicable after the record was made, it was read to the person in the language used by him or her during questioning and a copy of the record was made available to the person; and

(iii) the person was given the opportunity to interrupt the reading at any time for the purpose of drawing attention to any error or omission that he or she claimed had been made in or from the record and, at the end of the reading, the person was given the opportunity to state whether he or she claimed that there were any errors in or omissions from the record in addition to any to which he or she had drawn attention in the course of the reading; and

(iv) a tape recording was made of the reading referred to in subparagraph (ii) and of everything said by or to the person as a result of compliance

with subparagraph (iii), and the requirements of subsection (2) were observed in respect of that recording; and

(v) before the reading referred to in subparagraph (ii), an explanation, in accordance with the form in the Schedule, was given to the person of the procedure that would be followed for the purposes of compliance with that subparagraph and subparagraphs (iii) and (iv).

(2) If the questioning, confession or admission, or the confirmation of a confession or admission, of a person is recorded as required under this section, the investigating official must, without charge:

(a) if the recording is an audio recording only or a video recording only—make the recording or a copy of it available to the person or his or her legal representative within 7 days after the making of the recording; and

(b) if both an audio recording and a video recording were made—make the audio recording or a copy of it available to the person or his or her legal representative within 7 days after the making of the recording, and inform the person or his or her legal representative that an opportunity will be provided, on request, for viewing the video recording; and

(c) if a transcript of the tape recording is prepared—make a copy of the transcript available to the person or his or her legal representative within 7 days after the preparation of the transcript.

(3) 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.

(4) Despite any arrangement made under the *Commonwealth Places (Application of Laws) Act 1970*, this section applies to any offence under a law applied by that Act if the investigating official is a member or special member of the Australian Federal Police.

(5) A court may admit evidence to which this section applies even if the requirements of this section have not been complied with, or there is insufficient evidence of compliance with those requirements, if, having regard to the nature of and the reasons for the non-compliance or insufficiency of evidence and any other relevant matters, the court is satisfied that, in the special circumstances of the case, admission of the evidence would not be contrary to the interests of justice.

(6) A court may admit evidence to which this section applies even if a provision of subsection (2) has not been complied with if, having regard to the reasons for the non-compliance and any other relevant matters, the court is satisfied that it was not practicable to comply with that provision.

(6A) To avoid doubt, subsection (6) does not limit subsection (5).

(7) If a judge permits evidence to be given before a jury under subsection (5) or (6), the judge must inform the jury of the non-compliance with the requirements of this section, or of the absence of sufficient evidence of compliance with those requirements, and give the jury such warning about the evidence as he or she thinks appropriate in the circumstances.

Part VI—Offences by and against public officers

Section 70—Disclosure of information by Commonwealth officers

(1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he is authorized to publish or communicate it, any fact or document which comes to his knowledge, or into his possession, by virtue of being a Commonwealth officer, and which it is his duty not to disclose, shall be guilty of an offence.

(2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him), any fact or document which came to his knowledge, or into his possession, by virtue of having been a Commonwealth officer, and which, at the time when he ceased to be a Commonwealth officer, it was his duty not to disclose, shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

Part VII—Official secrets and unlawful soundings

Section 78—Espionage and similar activities

Section 78 was repealed in 2002 and replaced in somewhat different terms by s 91.1 of the *Criminal Code Act 1995* (Cth) set out below by the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth).

However, it is relevant to the proceedings in *R v Lappas* as the accused were charged under s 78 (as well as under s 79(3) of the *Crimes Act 1914* (Cth)). Section 78 is set out in full in the discussion of *R v Lappas* in Appendix 4 at [12].

Section 79—Official secrets

(1) For the purposes of this section, a sketch, plan, photograph, model, cipher, note, document, or article is a prescribed sketch, plan, photograph, model, cipher, note, document or article in relation to a person, and information is prescribed information in relation to a person, if the person has it in his possession or control and:

(a) it has been made or obtained in contravention of this Part or in contravention of section 91.1 of the Criminal Code;

(b) it has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he has made or obtained it owing to his position as a person:

(i) who is or has been a Commonwealth officer;

(ii) who holds or has held office under the Queen;

(iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;

(iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or

(v) acting with the permission of a Minister;

and, by reason of its nature or the circumstances under which it was entrusted to him or it was made or obtained by him or for any other reason, it is his duty to treat it as secret; or

(c) it relates to a prohibited place or anything in a prohibited place and:

(i) he knows; or

(ii) by reason of its nature or the circumstances under which it came into his possession or control or for any other reason, he ought to know;

that it should not be communicated to a person not authorized to receive it.

(2) If a person with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions:

(a) communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:

(i) a person to whom he is authorized to communicate it; or

(ii) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his duty to communicate it;

or permits a person, other than a person referred to in subparagraph (i) or (ii), to have access to it;

(b) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it; or

(c) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article;

he shall be guilty of an indictable offence.

Penalty: Imprisonment for 7 years.

(3) If a person communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:

(a) a person to whom he is authorized to communicate it; or

(b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his duty to communicate it;

or permits a person, other than a person referred to in paragraph (a) or (b), to have access to it, he shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

(4) If a person:

(a) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it;

(b) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article; or

(c) fails to take reasonable care of a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, or to ensure that it is not communicated to a person not authorized to receive it or so conducts himself as to endanger its safety;

he shall be guilty of an offence.

Penalty: Imprisonment for 6 months.

(5) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing or having reasonable ground to believe, at the time when he receives it, that it is communicated to him in contravention of section 91.1 of the Criminal Code or subsection (2) of this section, he shall be guilty of an indictable offence unless he proves that the communication was contrary to his desire.

Penalty: Imprisonment for 7 years.

(6) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing, or having reasonable ground to believe, at the time when he receives it, that it is communicated to him in contravention of subsection (3), he shall be guilty of an offence unless he proves that the communication was contrary to his desire.

Penalty: Imprisonment for 2 years.

(7) On a prosecution under subsection (2) it is not necessary to show that the accused person was guilty of a particular act tending to show an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions and, notwithstanding that such an act is not proved against him, he may be convicted if, from the circumstances of the case, from his conduct or from his known character as proved, it appears that his intention was to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions.

(8) On a prosecution under this section, evidence is not admissible by virtue of subsection (7) if the magistrate exercising jurisdiction with respect to the examination and commitment for trial of the defendant, or the judge presiding at the trial, as the case may be, is of the opinion that that evidence, if admitted:

(a) would not tend to show that the defendant intended to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions; or

(b) would, having regard to all the circumstances of the case and notwithstanding subsection (9), prejudice the fair trial of the defendant.

(9) If evidence referred to in subsection (8) is admitted at the trial, the judge shall direct the jury that the evidence may be taken into account by the jury only on the question whether the defendant intended to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions and must be disregarded by the jury in relation to any other question.

(10) A person charged with an offence against subsection (2) may be found guilty of an offence against subsection (3) or (4) and a person charged with an offence against subsection (5) may be found guilty of an offence against subsection (6).

Section 85B—Hearing in camera etc.

(1) At any time before or during the hearing before a federal court, a court exercising federal jurisdiction or a court of a Territory of an application or other proceedings, whether in pursuance of this Act or otherwise, the judge or magistrate, or other person presiding or competent to preside over the proceedings, may, if satisfied that such a course is expedient in the interest of the defence of the Commonwealth:

(a) order that some or all of the members of the public shall be excluded during the whole or a part of the hearing of the application or proceedings;

(b) order that no report of the whole or a specified part of or relating to the application or proceedings shall be published; or

(c) make such order and give such directions as he thinks necessary for ensuring that no person, without the approval of the court, has access, either before, during or after the hearing of the application or the proceedings, 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.

(2) A person who contravenes or fails to comply with an order made or direction given in pursuance of this section shall be guilty of an offence.

Penalty: Imprisonment for 5 years.

Criminal Code Act 1995 (Cth)

Division 91—Offences relating to espionage and similar activities

Section 91.1—Espionage and similar activities

(1) A person commits an offence if:

(a) the person communicates, or makes available:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so intending to prejudice the Commonwealth's security or defence; and

(c) 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.

Penalty: Imprisonment for 25 years.

(2) A person commits an offence if:

(a) the person communicates, or makes available:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) without lawful authority; and

(ii) intending to give an advantage to another country's security or defence; and

(c) 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.

Penalty: Imprisonment for 25 years.

(3) A person commits an offence if:

(a) the person makes, obtains or copies a record (in any form) of:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and

(ii) intending to prejudice the Commonwealth's security or defence.

Penalty: Imprisonment for 25 years.

(4) A person commits an offence if:

(a) the person makes, obtains or copies a record (in any form) of:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) without lawful authority; and

(ii) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and

(iii) intending to give an advantage to another country's security or defence.

Penalty: Imprisonment for 25 years.

(5) For the purposes of subparagraphs (3)(b)(i) and (4)(b)(ii), the person concerned does not need to have a particular country, foreign organisation or person in mind at the time when the person makes, obtains or copies the record.

(6) A person charged with an offence under this section may only be remanded on bail by a judge of the Supreme Court of a State or Territory. This subsection has effect despite anything in section 93.1.

Note: Section 93.1 deals with how a prosecution is instituted.

(7) Section 15.4 of the Criminal Code (extended geographical jurisdiction—category D) applies to offences under this section.

Division 93—Prosecutions and hearings

Section 93.2—Hearing in camera etc.

(1) This section applies to a hearing of an application or other proceedings before a federal court, a court exercising federal jurisdiction or a court of a Territory, whether under this Act or otherwise.

(2) At any time before or during the hearing, the judge or magistrate, or other person presiding or competent to preside over the proceedings, may, 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.

(3) A person commits an offence if the person contravenes an order made or direction given under this section.

Penalty: Imprisonment for 5 years.

Defence Force Discipline Act 1982 (Cth)

Section 58—Unauthorised disclosure of information

(1) A person who is a defence member or a defence civilian is guilty of an offence if:

(a) the person discloses information; and

(b) there is no lawful authority for the disclosure; and

(c) the disclosure is likely to be prejudicial to the security or defence of Australia.

Maximum punishment: Imprisonment for 2 years.

(2) Strict liability applies to paragraph (1)(c).

Note: For strict liability, see section 6.1 of the Criminal Code.

(3) It is a defence if the person proves that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to be prejudicial to the security or defence of Australia.

Note: The defendant bears a legal burden in relation to the matter in subsection (3). See section 13.4 of the Criminal Code.

Evidence Act 1995 (Cth)

Part 3.10—Privileges

Division 3—Evidence excluded in the public interest

Section 130—Exclusion of evidence of matters of state

(1) 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.

(2) The court may give such a direction either on its own initiative or on the application of any person (whether or not the person is a party).

(3) In deciding whether to give such a direction, the court may inform itself in any way it thinks fit.

(4) Without limiting the circumstances in which information or a document may be taken for the purposes of subsection (1) to relate to matters of state, the information or document is taken for the purposes of that subsection to relate to matters of state if adducing it as evidence would:

(a) prejudice the security, defence or international relations of Australia; or

(b) damage relations between the Commonwealth and a State or between 2 or more States; or

(c) prejudice the prevention, investigation or prosecution of an offence; or

(d) prejudice the prevention or investigation of, or the conduct of proceedings for recovery of civil penalties brought with respect to, other contraventions of the law; or

(e) disclose, or enable a person to ascertain, the existence or identity of a confidential source of information relating to the enforcement or administration of a law of the Commonwealth or a State; or

(f) prejudice the proper functioning of the government of the Commonwealth or a State.

(5) Without limiting the matters that the court may take into account for the purposes of subsection (1), it is to take into account the following matters:

(a) the importance of the information or the document in the proceeding;

(b) if the proceeding is a criminal proceeding—whether the party seeking to adduce evidence of the information or document is a defendant or the prosecutor;

(c) the nature of the offence, cause of action or defence to which the information or document relates, and the nature of the subject matter of the proceeding;

(d) the likely effect of adducing evidence of the information or document, and the means available to limit its publication;

(e) whether the substance of the information or document has already been published;

(f) if the proceeding is a criminal proceeding and the party seeking to adduce evidence of the information or document is a defendant—whether the direction is to be made subject to the condition that the prosecution be stayed.

(6) A reference in this section to a State includes a reference to a Territory.

Section 134—Inadmissibility of evidence that must not be adduced or given

Evidence that, because of this Part, must not be adduced or given in a proceeding is not admissible in the proceeding.

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

Section 34—Secrecy

(1) Subject to subsection (1A), a person who is, or has at any time been, the Inspector-General or a member of the staff of the Inspector-General or who is acting, or has at any time acted, as the Inspector-General or as a member of the staff of the Inspector-General shall not, either directly or indirectly, except in the performance of his or her functions or duties or in the exercise of his or her powers under this Act:

(a) make a record of, or divulge or communicate to any person, any information acquired by reason of the person holding, or acting in, that office; or

(b) make use of any such information.

Penalty: $5,000 or imprisonment for 2 years, or both.

(1A) Subsection (1) does not apply if the Inspector-General:

(a) believed on reasonable grounds that the making of the record, or the divulging, communicating or use of the information (the conduct) by the person mentioned in subsection (1) is necessary for the purpose of preserving the well-being or safety of another person; and

(b) authorised the person mentioned in subsection (1) to engage in the conduct for that purpose.

(2) An offence against subsection (1) is an indictable offence.

(3) Notwithstanding that an offence against subsection (1) is an indictable offence, a court of summary jurisdiction may hear and determine proceedings in respect of such an offence if the court is satisfied that it is appropriate to do so and the defendant and the prosecutor consent.

(4) Where, in accordance with subsection (3), a court of summary jurisdiction convicts a person of an offence against subsection (1), the penalty that the court may impose is a fine not exceeding $2,000 or imprisonment for a period not exceeding one year, or both.

(5) A person who is, or has at any time been, the Inspector-General or a member of the staff of the Inspector-General or who is acting, or has at any time acted, as the Inspector-General or as a member of the staff of the Inspector-General shall not be required to produce in a court any document of which the person has custody, or to which the person has access, by reason of the person's office or employment under or for the purposes of this Act, or to divulge or communicate to a court any information obtained by the person by reason of that office or employment, except where it is necessary to do so for the purposes of this Act.

(6) In this section:

court includes any tribunal, authority or person having power to require the production of documents or the answering of questions.

produce includes permit access to.

(7) A reference in this section to information or a document shall be read as a reference to information or a document supplied for the purposes of this Act.

Intelligence Services Act 2001 (Cth)

Section 39—Communication of certain information—ASIS

(1) A person is guilty of an offence if:

(a) the person communicates any information or matter that was prepared by or on behalf of ASIS in connection with its functions or relates to the performance by ASIS of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member or agent of ASIS; or

(ii) his or her having entered into any contract, agreement or arrangement with ASIS; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and

(c) the communication was not made:

(i) to the Director-General or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director-General or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member or agent, within the limits of authority conferred on the person by the Director-General; or

(iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

Section 40—Communication of certain information—DSD

(1) A person is guilty of an offence if:

(a) the person communicates any information or matter that was prepared by or on behalf of DSD in connection with its functions or relates to the performance by DSD of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of DSD; or

(ii) his or her having entered into any contract, agreement or arrangement with DSD; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DSD; and

(c) the communication was not made:

(i) to the Director or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director; or

(iv) with the approval of the Director or of a staff member having the authority of the Director to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

Public Service Act 1999 (Cth)

Section 10—APS Values

(1) The APS Values are as follows:

(a) the APS is apolitical, performing its functions in an impartial and professional manner;

(b) the APS is a public service in which employment decisions are based on merit;

(c) the APS provides a workplace that is free from discrimination and recognises and utilises the diversity of the Australian community it serves;

(d) the APS has the highest ethical standards;

(e) the APS is openly accountable for its actions, within the framework of Ministerial responsibility to the Government, the Parliament and the Australian public;

(f) the APS is responsive to the Government in providing frank, honest, comprehensive, accurate and timely advice and in implementing the Government's policies and programs;

(g) the APS delivers services fairly, effectively, impartially and courteously to the Australian public and is sensitive to the diversity of the Australian public;

(h) the APS has leadership of the highest quality;

(i) the APS establishes workplace relations that value communication, consultation, co-operation and input from employees on matters that affect their workplace;

(j) the APS provides a fair, flexible, safe and rewarding workplace;

(k) the APS focuses on achieving results and managing performance;

(l) the APS promotes equity in employment;

(m) the APS provides a reasonable opportunity to all eligible members of the community to apply for APS employment;

(n) the APS is a career-based service to enhance the effectiveness and cohesion of Australia's democratic system of government;

(o) the APS provides a fair system of review of decisions taken in respect of APS employees.

(2) For the purposes of paragraph (1)(b), a decision relating to engagement or promotion is based on merit if:

(a) an assessment is made of the relative suitability of the candidates for the duties, using a competitive selection process; and

(b) the assessment is based on the relationship between the candidates' work-related qualities and the work-related qualities genuinely required for the duties; and

(c) the assessment focuses on the relative capacity of the candidates to achieve outcomes related to the duties; and

(d) the assessment is the primary consideration in making the decision.

Section 13—The APS Code of Conduct

(1) An APS employee must behave honestly and with integrity in the course of APS employment.

(2) An APS employee must act with care and diligence in the course of APS employment.

(3) An APS employee, when acting in the course of APS employment, must treat everyone with respect and courtesy, and without harassment.

(4) An APS employee, when acting in the course of APS employment, must comply with all applicable Australian laws. For this purpose, Australian law means:

(a) any Act (including this Act), or any instrument made under an Act; or

(b) any law of a State or Territory, including any instrument made under such a law.

(5) 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.

(6) An APS employee must maintain appropriate confidentiality about dealings that the employee has with any Minister or Minister's member of staff.

(7) An APS employee must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with APS employment.

(8) An APS employee must use Commonwealth resources in a proper manner.

(9) An APS employee must not provide false or misleading information in response to a request for information that is made for official purposes in connection with the employee's APS employment.

(10) An APS employee must not make improper use of:

(a) inside information; or

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

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

(11) An APS employee must at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.

(12) An APS employee on duty overseas must at all times behave in a way that upholds the good reputation of Australia.

(13) An APS employee must comply with any other conduct requirement that is prescribed by the regulations.

Section 15—Breaches of the Code of Conduct

(1) An Agency Head may impose the following sanctions on an APS employee in the Agency who is found (under procedures established under subsection (3)) 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.

(2) The regulations may prescribe limitations on the power of an Agency Head to impose sanctions under subsection (1).

(3) An Agency Head must establish procedures for determining whether an APS employee in the Agency has breached the Code of Conduct. The procedures:

(a) must comply with basic procedural requirements set out in Commissioner's Directions; and

(b) must have due regard to procedural fairness; and

(c) may be different for different categories of APS employees.

(4) The Commissioner must issue directions in writing for the purposes of subsection (3).

(5) An Agency Head must take reasonable steps to ensure that every APS employee in the Agency has ready access to the documents that set out the procedures referred to in subsection (3).

Public Service Regulations

Regulation 7

(13) An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head's express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.

United States Constitution

Article III

Section 1.
The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

Section 2.
Clause 1: The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public Ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States,—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

Clause 2: In all Cases affecting Ambassadors, other public Ministers and Consuls, and those in which a State shall be Party, the supreme Court shall have original Jurisdiction. In all the other Cases before mentioned, the supreme Court shall have appellate

Jurisdiction, both as to Law and Fact, with such Exceptions, and under such Regulations as the Congress shall make.

Clause 3: The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed.

First Amendment

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.

Fourth Amendment

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.

Sixth Amendment

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.

International Convention on Civil and Political Rights

Article 4

1. In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.
2. No derogation from articles 6, 7, 8 (paragraphs 1 and 2), 11, 15, 16 and 18 may be made under this provision.
3. Any State Party to the present Covenant availing itself of the right of derogation shall immediately inform the other States Parties to the present Covenant, through the intermediary of the Secretary-General of the United Nations, of the provisions from which it has derogated and of the reasons by which it was actuated. A

further communication shall be made, through the same intermediary, on the date on which it terminates such derogation.

Article 14

1. All persons shall be equal before the courts and tribunals. 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 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 requires, 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 judgement 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.

2. Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

3. In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality:

   (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;

   (c) To be tried without undue delay;

   (d) To be tried in his presence, and to defend himself in person or through legal assistance of his own choosing; to be informed, 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;

   (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;

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

4. In the case of juvenile persons, the procedure shall be such as will take account of their age and the desirability of promoting their rehabilitation.

5. Everyone convicted of a crime shall have the right to his conviction and sentence being reviewed by a higher tribunal according to law.

6. When a person has by a final decision been convicted of a criminal offence and when subsequently his conviction has been reversed or he has been pardoned on the ground that a new or newly discovered fact shows conclusively that there has been a miscarriage of justice, the person who has suffered punishment as a result of such conviction shall be compensated according to law, unless it is proved that the non-disclosure of the unknown fact in time is wholly or partly attributable to him.

7. No one shall be liable to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country.

Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

   (a) For respect of the rights or reputations of others;

   (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

European Convention on Human Rights

Article 6

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly by the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

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

   (b) to have adequate time and the facilities for the preparation of his defence;

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

(d) 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;

(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 10

1. Everyone has the right to freedom of expression. this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Appendix 4. *R v Lappas*

1. The prosecution of Simon Lappas and Sherryll Dowling is important in understanding the issues that gave rise to this inquiry. Indeed, the outcome of those proceedings at first instance was probably the immediate prompt to the Australian Government to issue the Terms of Reference for this inquiry. The case's importance also lies in the fact that it appears to be one of only three prosecutions to date under Australia's counter-espionage criminal law, the others being *Grant v Headland*[1] and the prosecution of George Sadil in 1994.[2]

2. Understandably, only limited information is available about the proceedings against Lappas and Dowling. To date, only two judgments have been published:

- the Reasons for Ruling issued by the trial judge, Gray J, in the Supreme Court of the Australian Capital Territory on 26 November 2001 in relation to the Crown's application for public interest immunity over some of the documents that were at the centre of the charges;[3] and

- the judgment of the Court of Appeal of the Australian Capital Territory in the Crown's appeal on sentence delivered on 23 October 2003.[4]

3. In this Appendix, the description of the factual background of the case comes very largely from the Court of Appeal's judgment and the discussion of the procedural issues comes largely from the trial judge's Reasons for Ruling. The remainder comes principally from reports in *The Canberra Times*, highlighting perhaps the major role that the media can play in the proper dissemination of important information.

4. It is apparent why some of the details of the evidence in the case could not be made public. The trial judge and Court of Appeal were clearly conscious of the need to be circumspect in wording their published judgments and in sealing those that have not been published. The fact that the case cannot be published in full naturally restricts the benefit that might be derived from it, especially given that so few such cases reach Australian courts.

---

1 *Grant v Headland* (1977) 17 ACTR 29, which also involved a charge under s 79 of the *Crimes Act 1914*, but not under s 78.
2 See Ch 8 at [8.40] and [8.231] above.
3 *R v Lappas and Dowling* [2001] ACTSC 115.
4 *R v Lappas* [2003] ACTCA 21.

Factual background

5. Lappas graduated from university with a science degree in 1997, aged 22. Two years later he was employed by the Defence Intelligence Organisation (DIO) as a probationary intelligence officer. His duties involved the assessment of information in relation to military technology, and he was cleared to have access to material classified as Top Secret, the highest of the national security information classifications set out in the *Commonwealth Protective Security Manual* (PSM).[5] In April 2000, he was directed to prepare a report based on certain information which, though unclassified, would have warranted a Secret classification, the second-highest national security information classification.[6] The report was marked Top Secret and AUSTEO (for Australian Eyes Only).[7]

6. On 6 July 2000, Lappas met Sherryll Dowling. They met again on 9 July and spent the next day together.

7. On 11 July, Lappas went to work and took the report that he had been drafting in order to give it to Dowling so that she could sell it to a particular foreign power that Lappas thought would be willing to pay a significant amount. He also gave her detailed instructions about how to go about selling it. Before giving it to her, Lappas made some handwritten annotations to it which were more sensitive than the material in the draft report itself, and gave the names of two people who had given Australian intelligence agencies information about the foreign power, and were expected to do so again in the future. Later that day Lappas contacted the foreign power himself to facilitate the sale of the report, without success.

8. On the following day, Dowling tried to sell the document to the foreign power, also without success. That same day, Lappas photocopied two Top Secret documents which apparently originated from another foreign power. He gave the copies to Dowling so that she could sell them with the report. Lappas tried to sell the documents for her that evening, but again failed.

9. Two days later (on a Friday), Lappas informed a colleague what he had done and was told that he should inform the DIO security officer. Lappas tried to do so, unsuccessfully. Later that evening, he told another colleague what he had done and was told that he should try to get the documents back over the weekend. On the following day, Saturday, Lappas told Dowling to expect a visit from the authorities, to burn the report and to hand the other two documents to the police. On the Sunday, the second

---

5 Attorney-General's Department, *Commonwealth Protective Security Manual* (2000), C 30–32 [6.26]–[6.34].

6 This would presumably have fallen within the meaning of the expression 'security sensitive information' as used by the Attorney-General's Department in the Terms of Reference for this inquiry: see Ch 1.

7 D McLennan, 'Top-Secret Documents Withheld from Jury', *The Canberra Times*, 20 November 2001. At the trial, this was described as a three-page report of an interview, nine pages of emails in a foreign language and a cover sheet classified as Security-in-Confidence: R Campbell, 'Nation's Security "Not Threatened"', *The Canberra Times*, 14 May 2002.

colleague in whom Lappas had confided told him that he must report the matter by the following day or the colleague would do so. Lappas arranged to meet the DIO security officer that night. He confessed, but appeared so distressed that he spent that night at the security officer's home. He went to the DIO the next morning with the security officer and informed the senior management what he had done. A day later, police recovered all three documents from Dowling.

10. During the videotaped interview by police, Lappas's solicitor was required to turn his back for long periods since he was not permitted to see the documents about which the police were questioning his client.[8]

11. Ultimately, a large amount of evidence was presented to the Court about Lappas's psychological condition—which, though highly relevant to sentencing and to an understanding of his motivation, is not widely discussed in the published judgments, though it is given more attention in the media reports. He was described as having had a history of depression and a failing seven-year engagement.[9]

Charges

12. In July 2000, Lappas was charged with offences under s 79(3) of the *Crimes Act 1914* (Cth).[10] Additional charges under s 78(1)(b) were brought in 2001. Dowling was also charged under s 79. Section 78 read:[11]

> **78 Espionage and similar activities**
>
> (1) If a person with the intention of prejudicing the safety or defence of the Commonwealth or a part of the Queen's dominions:
>
> (a) makes a sketch, plan, photograph, model, cipher, note, document or article that is likely to be, might be or is intended to be directly or indirectly useful to an enemy or a foreign power;
>
> (b) obtains, collects, records, uses, has in his possession or communicates to another person a sketch, plan, photograph, model, cipher, note, document, article or information that is likely to be, might be or is intended to be directly or indirectly useful to an enemy or a foreign power; or
>
> (c) approaches, is in the neighbourhood of, is in, enters, inspects or passes over a prohibited place;
>
> he shall be guilty of an indictable offence.
>
> Penalty: Imprisonment for 7 years.

---

8 R Campbell, 'Nation's Security "Not Threatened"', *The Canberra Times*, 14 May 2002.

9 R Campbell, 'Spy Case: "No Intent" in Passing Documents', *The Canberra Times*, 14 May 2002.

10 The current version of s 79 is set out in Appendix 3. It was amended in 2002—after the events in *Lappas* took place—but only by replacing the words 'safety or defence' throughout with the words 'defence or security': *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth), Sch 1.

11 Section 78 was subsequently repealed and replaced (though not in identical terms) by s 91.1 of the *Criminal Code Act 1995* (Cth), which is set out in Appendix 3.

> (2) On a prosecution under this section:
>
> (a) it is not necessary to show that the accused person was guilty of a particular act tending to show an intention to prejudice the safety or defence of the Commonwealth or a part of the Queen's dominions and, notwithstanding that such an act is not proved against him, he may be convicted if, from the circumstances of the case, from his conduct or from his known character as proved, it appears that his intention was to prejudice the safety or defence of the Commonwealth or a part of the Queen's dominions; and
>
> (b) if any sketch, plan, photograph, model, cipher, note, document, article or information relating to or used in a prohibited place, or anything in such a place, was made, obtained, collected, recorded, used, possessed or communicated by any person other than a person acting under lawful authority, it shall, unless the contrary is proved, be deemed to have been made, obtained, collected, recorded, used, possessed or communicated with the intention of prejudicing the safety or defence of the Commonwealth or a part of the Queen's dominions.
>
> (3) On a prosecution under this section, evidence is not admissible by virtue of paragraph (2)(a) if the magistrate exercising jurisdiction with respect to the examination and commitment for trial of the defendant, or the judge presiding at the trial, as the case may be, is of the opinion that that evidence, if admitted:
>
> (a) would not tend to show that the defendant intended to prejudice the safety or defence of the Commonwealth or a part of the Queen's dominions; or
>
> (b) would, having regard to all the circumstances of the case and notwithstanding subsection (4), prejudice the fair trial of the defendant.
>
> (4) If evidence referred to in subsection (3) is admitted at the trial, the judge shall direct the jury that the evidence may be taken into account by the jury only on the question whether the defendant intended to prejudice the safety or defence of the Commonwealth or a part of the Queen's dominions and must be disregarded by the jury in relation to any other question.

13. The charge under s 78(1)(b) was described by Higgins CJ in the ACT Court of Appeal as 'inherently more serious' than that under s 79(3).[12] The element of intention to prejudice the safety or defence of the Commonwealth is presumed under s 78, unless the contrary is proved.[13] No charges were laid under s 79(2), though this appears to have been open to the Crown.

14. Under s 78(1), the Crown bore the onus of proving that the documents were passed with the intention of them being 'directly or indirectly useful' to a foreign power, which put the contents of the documents directly in issue.[14] Lappas consistently

12 *R v Lappas* [2003] ACTCA 21, [8].
13 Ibid, [9].
14 *R v Lappas and Dowling* [2001] ACTSC 115, [20].

denied that he had had any intention to prejudice the defence or safety of the Commonwealth.

Claims for secrecy and state interest immunity

15. All documents passed by Lappas to Dowling were tendered as evidence, in camera, at the committal hearing in April 2001, which was before a magistrate without a jury. Lappas's defence counsel were given access to them at that time. The ALRC understands that senior counsel representing Lappas at this time held a security clearance.

16. In September 2001 the Crown applied unsuccessfully to have the whole of the trial conducted in camera. However, the trial judge ordered the public to be excluded when the proceedings would disclose:

- the contents of the documents which were the subject of the charges;
- the source of the information in those documents;
- details of Lappas's work at the DIO;
- details of the activities of defence agencies;
- details of witnesses employed by the DIO; and
- the identity, and relationship with the DIO, of any witness.

17. The prosecution was directed to identify and notify the defence of those witnesses and the evidence caught by these orders; the defence was directed to respond and nominate any other evidence that should be heard in closed court. Media organisations were given an opportunity to address the court on these orders.[15]

18. Lappas and Dowling's trials were ordered to be heard separately.[16]

19. At Lappas's trial in November 2001, the Crown declined to tender as evidence the two documents sourced from a foreign power.[17] Rather the prosecutors sought to tender 'blacked out' versions of the documents and to lead oral evidence that would describe their character in general terms. The Crown had hoped to obtain the defence's consent to this approach, which was not forthcoming. When Lappas's defence counsel sought to tender the documents after cross-examining a prosecution witness on them,

---

15 D McLennan, 'Spying Case: Bid for Total Secrecy Rejected', *The Canberra Times*, 11 September 2001.

16 R Campbell, 'Espionage Trials to be Held Separately', *The Canberra Times*, 20 December 2001.

17 Though, oddly, it was later reported that the prosecution had conceded that they were 'innocuous': R Campbell, 'I Was Told to Burn Document: Woman', *The Canberra Times*, 10 December 2002. This seems improbable.

the Crown made its first claim for state interest immunity under s 130 of the *Evidence Act 1995* (Cth). Subsection 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.[18]

20. The Crown indicated that it intended to lead very limited oral evidence of the general description of the contents of the documents, without actually revealing their contents. Gray J observed that the very general summary of the sensitive material given to him, together with copies of the documents with significant portions blacked out, would not have allowed him to draw the inferences that the prosecution required him to draw as part of its case.[19]

21. In any event, the approach proposed by the Crown was not open to it as s 134 of the *Evidence Act* prevented any evidence of material that is the subject of state interest immunity being admitted into evidence.[20]

22. The trial judge granted the application to accord state interest immunity to the two highly sensitive documents but ruled that to do so would hinder the defence's ability to adduce evidence before the jury on the question of the document's usefulness to a foreign power, and concluded the accused would not get a fair trial under these circumstances. Accordingly, he stayed the prosecution in relation to these two documents brought under s 78. Lappas and Dowling's trials on the remaining charges relating to these two documents and the annotated report proceeded at a later date in May 2002.

23. The ALRC understands that the foreign power that was the source of the two highly sensitive documents refused to allow them to be tendered in open court or to allow access to them by anyone without a security clearance to the requisite level. It must be borne in mind that federal indictable offences, such as those with which Lappas and Dowling were charged, must be tried before a jury, as required by s 80 of the *Australian Constitution*.[21]

24. The trial judge found it 'regrettable' that the claim for state interest immunity was not made at the committal proceedings since, if it had, the prosecution may have been able to proceed in a different way.[22]

25. Lappas's trial resumed in May 2002—but in its seventh day was again aborted after Lappas's legal representatives withdrew due to what was described as 'ethical

---

18 Section 130 is set out in Appendix 3.
19 *R v Lappas and Dowling* [2001] ACTSC 115, [8]–[9].
20 Section 134 is set out in Appendix 3.
21 Section 80 is set out in Appendix 3.
22 *R v Lappas and Dowling* [2001] ACTSC 115, [18]–[19].

difficulties'.[23] Up to that point, Lappas had been on bail since his arrest in July 2000. The Crown apparently applied for bail to be revoked in an in-camera hearing, which the trial judge acceded to and remanded Lappas in custody without any public explanation. The jury was discharged but reminded by the judge that they were 'forbidden to say anything about much of the evidence or the witnesses'.[24] The judgment of the Court of Appeal indicates that Lappas served eight days in remand.[25]

26. It was later reported that the trial had been aborted because Lappas had threatened to reveal classified information to a foreign power.[26] A raid on Lappas's Canberra home failed to reveal anything[27] and his counsel later submitted that this 'threat' may have been a reflection of his client's fragile mental state.

27. It was reported that Dowling's name was suppressed at Lappas's aborted trial in May 2002[28] and again when it recommenced in November 2002.[29] However, this could well have been with a view to avoid prejudicing her trial, which was to follow his, rather than out of concern for national security.[30]

Confidentiality undertakings

28. Shortly after the withdrawal of his previous legal representatives, Lappas retained a new solicitor and counsel. The new senior and junior counsel and their instructing solicitor did not hold security clearances and declined to seek them in the face of a claim by the Crown that these checks had to be made.

29. Ultimately, Lappas's lawyers each gave undertakings to the Court in the following terms:

> I … hereby **undertake**:
>
> (a) to provide an appropriate level of protection, in accordance with the requirements of the Commonwealth *Protective Security Manual*, to the contents of all materials which have been identified as containing national security classified material, including the contents of any document led *in camera* or evidence of any *in camera* hearing contained in the transcript;
>
> (b) not to communicate, release, pass on, or enable access to information concerning the content of any of the material identified in paragraph (a) to any other

---

23 R Campbell, *Judge Aborts Lappas Trial*, <http://canberra.yourguide.com.au/detail.asp?story_id=150391&y=2002&m=5&class=News&subclass=Local&category=General+News&class_id=7> at 22 May 2002.
24 Ibid.
25 *R v Lappas* [2003] ACTCA 21, [41], [56], [141].
26 R Campbell, 'Lappas Trial Aborted after Threat, Court Told', *The Canberra Times*, 29 May 2002.
27 Ibid.
28 R Campbell, 'Spy Case: "No Intent" in Passing Documents', *The Canberra Times*, 14 May 2002; R Campbell, 'I Was Told to Burn Document: Woman', *The Canberra Times*, 10 December 2002.
29 See [32] below.
30 See also R Campbell, 'Espionage Trials to be Held Separately', *The Canberra Times*, 20 December 2001.

person, including any person working for the solicitors or counsel, other than to the defendant, Simon Lappas, junior counsel [name], and solicitor [name];

(c) to take all appropriate steps to ensure that the material identified in paragraph (a) is not communicated to any person not authorised by the Commonwealth to receive it and to adopt appropriate handling procedures to ensure the safety of the material;

(d) to store the material identified in paragraph (a) and any notes containing information from that material in locked appropriate security containers at all times when the material is not is use;

(e) to return the material identified in paragraph (a) to the Commonwealth at the conclusion of the proceedings;

(f) to destroy any notes taken from the material identified in paragraph (a) in accordance with procedures for the destruction of national security classified material;

(g) not to record at any time any information from the material identified in paragraph (a) on any computer or computer systems which have not been approved by the Commonwealth for that purpose;

(h) in respect of the document which is the subject of the count on the indictment,[31] not to copy, take notes from, or make any attempt to reconstruct the contents of the document; and

hereby **acknowledge**:

(i) that I have had a briefing from the Australian Security Intelligence Organisation and the Department of Defence regarding obligations under the Commonwealth *Protective Security Manual* relating to the safe handling of national security classified material;

(j) that the Commonwealth has advised that I will not be given a copy of the document which is the subject of the count on the indictment but that access may be provided to inspect this document by prior arrangement with the Australian Federal Police;

(k) that the information contained within the material identified in paragraph (a) has been entrusted to me by the Commonwealth and that it is my duty to treat that information as secret; and

(l) that I am aware of the obligations set out in subsection 18(2) of the *Australian Security Intelligence Organisation Act 1979*[32] and section 79 of the *Crimes Act 1914*.[33]

---

31 The ALRC understands that this is a reference to the annotated report.

32 Section 18 is set out in Appendix 3.

33 *Undertaking given by Lex Lasry QC in The Commonwealth v Simon Lappas*, 2002. See also R Campbell, 'Lappas Trial Aborted after Threat, Court Told', *The Canberra Times*, 29 May 2002 and K Brine, 'Defence Team to Get Secret Papers', *The Canberra Times*, 11 July 2002.

30. These undertakings apparently did not satisfy the foreign power from which the two highly sensitive documents were sourced since it continued to refuse to permit them to be tendered in the proceedings.

31. The Crown conceded that the judge was exempt from the requirement to hold a security clearance. It also stated that, although the jurors were not cleared and therefore the relevant government agencies did not want them to see the sensitive documents, they had to so that the trial could proceed at all.[34]

The trial resumed

32. The trial resumed in November 2002. A newspaper report[35] indicates that Dowling's name had been suppressed although it had appeared in earlier reports and on the title of the trial judge's Reasons for Ruling issued in November 2001.[36] Again, the suppression of her name may have been to avoid any prejudice to her separate trial.[37] The same newspaper article also states that the name of a former DIO colleague of Lappas was suppressed although the names of two such colleagues appear in the Court of Appeal's judgment.[38]

33. The trial proceeded for 11 days and Lappas was found guilty by the jury of the offence under s 78(1)(b). He had previously pleaded guilty to the alternative offence under s 79(3) in relation to the report (which was made redundant for the purposes of sentencing by the jury's verdict) and in relation to the other two highly sensitive documents. The charge under s 78(1)(b) in relation to the two latter documents was the charge that was stayed by Gray J in November 2001.[39] Sentencing was delayed until January 2003 to allow time for psychiatric evidence to be compiled and presented.

Sentencing and appeal

34. Lappas was sentenced on 30 January 2003 to 12 months' imprisonment for the offence under s 78 (for which the maximum penalty was seven years' imprisonment) and to three months' imprisonment for the offence under s 79 relating to the two highly sensitive documents (for which the maximum penalty was two years' imprisonment), to be served concurrently. Both sentences were suspended upon Lappas entering into a two-year good behaviour bond.

35. The Crown appealed against the insufficiency of the sentence, and on 30 October 2003 the ACT Court of Appeal ordered that Lappas be imprisoned for two years and for six months respectively for the two offences, only three months of which were to be served concurrently, and to serve at least six months of those terms.

---

34 R Campbell, 'Spy Trial: Lawyers in Security Deadlock', *The Canberra Times*, 7 June 2002.
35 R Campbell, 'Lappas Near Emotional Collapse, Jury Told', *The Canberra Times*, 3 December 2002, 4.
36 *R v Lappas and Dowling* [2001] ACTSC 115.
37 See [27] above.
38 *R v Lappas* [2003] ACTCA 21, [66], [76], [77], [79].
39 See [19]–[24] above.

36. Lappas has sought special leave to appeal to the High Court of Australia. After spending three days in gaol, he was released on bail pending the hearing of his application for expedition of his application for special leave. Expedition was granted in December 2003 and the application for special leave is scheduled to be heard in March 2004.[40]

37. The published judgments do not reveal Dowling's fate but ASIO has reported that she pleaded guilty to two charges of receiving prescribed documents and on 9 May 2003 was placed on a five-year good behaviour bond.[41] She was not the subject of the Crown's appeal on sentence.

40 R Campbell, 'Progress Towards Early Hearing for Lappas', *The Canberra Times*, 3 December 2003, 13; R Campbell, 'High Court Grants Lappas Early Hearing of Application', *The Canberra Times*, 10 December 2003, 9.

41 Australian Security Intelligence Organisation, *Annual Report* (2003), 28.