Jill Hill
Barrister

Secrecy and Special Interest Immunity

Duty Not to Disclose Security Sensitive Information

Criminal Code Act 1995 (Cth)

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

Section 101 creates offences concerning terrorism, and in particular under section 101.5 makes it an offence to collect or make documents likely to facilitate terrorist acts.

Offences under the espionage and terrorism sections of the code carry heavy penalties; between 15 and 25 years imprisonment.

Crimes Act 1914 (Cth), s 79

Section 79 of the *Crimes Act 1914* (Cth) concerns unlawful disclosure of official secrets. The section contains a number of offences relating to the communication of official secrets to any person. A Commonwealth officer, or any person in receipt of information from a Commonwealth officer, may be guilty of an offence under this section.

Crimes Act 1914 (Cth), s 70

Under the *Crimes Act 1914* (Cth), s 70, a Commonwealth officer who discloses information obtained in the course of employment where there is a duty not to disclose it is guilty of an offence. This provision is cast very broadly. Unlike the espionage provisions in s 79, it does not distinguish between the disclosure of information that is harmful to the public interest and information that is not.

Australian Security Intelligence Organisation Act 1979 (Cth)

The Act provides a range of other safeguards to protect the disclosure of classified and security sensitive information.

Intelligence Services Act 2001 (Cth)

Under s 39 of the *Intelligence Services Act 2001*, any ASIS employee, agent or contractor who makes an unauthorized communication of information related to ASIS functions is guilty of an offence.

Public Service Act 1999 (Cth)

Section 13 of the *Public Service Act 1999* (Cth) sets out the Australian Public Service Code of Conduct, which binds APS employees, Agency Heads and statutory office holders. Among the requirements included in the Code of Conduct is that an employee must not make improper use of inside information.

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

Under the *Inspector-General of Intelligence and Security Act 1986* (Cth), personnel employed by the IGIS may not disclose, record or otherwise divulge information gathered in the course of their employment.

Defence Force Discipline Act 1982

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.

Strict liability applies to paragraph (1)

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 section13.4 of the Criminal Code.

Commonwealth Protective Security Manual

The Commonwealth Protective Security Manual is issued by the Commonwealth Attorney-General. It sets out minimum standards in protective security for all Commonwealth agencies, and for contractors and their employees who perform services for or on behalf of the Commonwealth. Part C of the manual deals with information security.

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.

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

Other key pieces of Australia's national security legislation include:

- The Anti-Terrorism Act 2004
- Australian Federal Police and Other Legislation Amendment Act 2004
- The Australian Protective Service Amendment Act 2003
- The Aviation Transport Security Act 2004
- The Border Security Legislation Amendment Act 2002

Public Interest Immunity

Common Law

The common law formulation of public interest immunity can be found in *Sankey v Whitlam* (1978) 142 CLR 1, 38, per Gibbs ACJ:

"[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."

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. What is required is a balancing of:

"[T]he nature of the injury which the nation or the public service would be likely to suffer, and the evidentiary value and importance of the documents in the particular litigation": Alister v The Queen (1983) 50 ALR 41 at 44 per Gibbs CJJ.

Public interest immunity can be distinguished from a privilege. 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: Issue Paper 28, ALRC.

Where public interest immunity is applied, all evidence related to the relevant secret is excluded, including any secondary evidence held by third parties: M Aronson and J Hunter, Litigation Evidence and Procedure (6th ed, 1998) Butterworths, at 597. 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": Cooke v Maxwell (1817) 171 ER 614, 615.

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.

Evidence Act 1995 (Cth)

Section 130 of the Evidence Act 1995 (Cth) provides that:

> (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.

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).

In deciding whether to give such a direction, the court may inform itself in any way it thinks fit.

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 prejudice the security, defence or international relations of Australia……..

The factors outlined are consistent with those developed by the prior common law. The ALRC noted in its report (ALRC 26, vol 1, paras 8640866):

> Research and enquiries have not revealed any serious inadequacies in the current common law approach…..It presently requires a balancing exercise, weighting the advantages of non-disclosure of information against the disadvantages….It is important to maintain the present supervisory role of the courts….”

In *State of NSW v Ryan* (1998) 101 LGERA 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[and the provisions of s 130.

Similarly, von Doussa J found in *Chapman v Luminis Pty Ltd* (No 2) (2000) 100 FCR 229 that the common law principles considered in *Aboriginal Sacred Sites Protection Authority v Maurice* (1986) 10 FCR 104 continued to apply under s 130.

Section 130(1) indicates that the onus is on the party arguing that the public interest in preserving secrecy or confidentiality that relates to matters of state to show that this factor outweighs the public interest in admitting into evidence the information or document.

This reflects the common law in that it does not confer absolute immunity on information relating to matters of state or an absolute right to protect the information, and appears to apply to both oral and documentary evidence: J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, at 469.

Mechanisms used to protect evidence governed by the statute are the same as under the common law:

- evidence taken in camera: *Scott v Scott* [1913] AC 417
- restriction of the publication of evidence
- suppressing the names of parties and witnesses: *R v Mr C* (1993) 67 A Crim R 562
- limiting access to evidence to a party’s legal advisors; *Church of Scientology of California v DHSS* [1979] 1 WLR 723 and
- granting absolute immunity.

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

The immunity provided by the Evidence Act only apply to information or a document that relates to "matters of state" and section 130 (4) specifically includes evidence which, if adduced, would:

"prejudice the security, defence or international relations of Australia".

It is essential to the application of the principles that the documents or evidence involved relate to the conduct of governmental functions: *R v Young* [1999] NSWCCA 166; 46 NSWLR 681.

The Act is in most respects a restatement of the common law, but it only applies to the admission of evidence. The common law still applies in pre-trial and proceedings contexts such as discovery, interrogatories and notices to produce whereas the Act applies to interlocutory proceedings, final hearings and on appeal. The exception to this is in civil proceedings in New South Wales, where the Supreme Court and District Court Rules specifically incorporate the principles to discovery, interrogatories, subpoenas, notices to produce and oral examination before officers of the court (similarly in the ACT Supreme Court Rules).

The ALRC has recently examined the operation of s 130 in the context of protection of classified and security sensitive information in court proceedings. In the Report *Keeping Secrets* (ALRC 98), it was estimated that public interest immunity arises as an issue in less than one per cent of cases across all courts. The ALRC also found that the public interest immunity procedure worked effectively, although the procedures for invoking its use were thought by some submittors to require clarification.

ALRC 26 had noted that one issue in relation to public interest immunity was whether some procedural provisions should be included in the uniform Evidence Acts to enable a judge's ruling to be obtained in advance of the trial, and to allow time for an appeal from that ruling. At the time of that Report, the ALRC considered that the decision in *Sankey v Whitlam* - 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.

Other Legislation

Special immunity – administrative decisions

Information relating to decisions of an administrative nature is not compellable under the Administrative Decisions (Judicial Review) Act if a certificate is issued by the Attorney-General on the basis that disclosure of the information would prejudice Australia's security, defence or international relations – eg (CTH) *Administrative Decisions (Judicial Review)* Act 1977 s 14(1)(a).

Ombudsman's Acts in all states generally overrides privilege immunity and secrecy obligations so that the Ombudsman can require the provision of information relating to matters he/she is investigating. The

exception to this power is where it has been certified that disclosure would prejudice security, defence or international relations – eg (CTH) Ombudsman Act 1976 s 9(3), 9(4), 9(5)

ICAC - generally, a witness summoned to appear is not entitled to refuse to answer any question put by the Commissioner or other presiding person, or to refuse to produce any document. In exercising its functions, the Commission shall regard the protection of the public interest and the prevention of breaches of public trust as its paramount concerns. This could conflict with national security considerations.

Security Considerations in Criminal Court Hearings:

The National Security Information (Criminal Proceedings) Act 2004 (Cth)

A defendant denied access to classified or security sensitive information upon which the prosecution relies may be able to argue that his or her right to a fair trial is compromised because of that denial and his or her consequent inability to challenge or test part of the evidence.

For example, in the prosecution of Simon Lappas, a former Defence Intelligence Organisation analyst, for passing classified information to an unauthorised person, the ACT Supreme Court upheld the prosecution's claim that certain documents not be disclosed on the basis of public interest immunity and ordered that they not be adduced as evidence but also stayed the relevant charge on the indictment. The Crown had 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."

His Honour concluded:

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

In January 2005 the National Security Information (Criminal Proceedings) Act 2004 came into force. It is largely a consequence of recommendations by the ALRC 98 for enhancing the regime for the protection of classified and security sensitive information through specific procedures, rather than by amending s 130 of the Evidence Act 1995 (Cth).

The object of the Act is to prevent the disclosure of information in federal court proceedings where the disclosure is likely to prejudice national security, "except to the extent that preventing the disclosure would seriously interfere with the administration of justice".

- "National security" is defined as Australia's defence, security, international relations or law enforcement interests.
- "Law enforcement interests" is defined very broadly and includes criminal intelligence, criminal investigation, foreign intelligence and security intelligence; protecting the technologies and methods used, protecting the safety of informants and of persons associated with informants.

The Act makes provision for management of issues relating to national security (and consequently "law enforcement interests") that may arise during the trial. It provides for pre-trial conferences and arrangements during the course of the trial, protection of

information disclosed during the trial, and post-trial protection, storage, handling and destruction of information.

For the Act to apply the prosecutor must first give notice in writing to the defendant, and the Act only applies to those parts of the proceedings that follow the written notice.

If either prosecutor or defendant knows or believes he or she or a witness will disclose information relating to national security (including his or her mere presence), that party must give notice in writing to the Attorney-General as soon as practicable, and must advise the court and other parties of the notice. Similarly, if a witness in the witness box is asked a question, and the prosecutor or defendant knows or believes the answer relates or may affect national security, the court is to be immediately advised and certain procedures follow culminating in notice being given to the Attorney General.

It is an offence for failure to give the Attorney General notice. The hearing must be adjourned pending the Attorney General's response.

The Attorney General, if he or she considers the evidence is likely to prejudice national security, may give a certificate to each potential discloser.

- **If the evidence is in the form of a document** the Attorney General may give permission to disclose none of the document, part only of the document, and/or a statement of the facts that the document would be likely to prove, and/or the circumstances in which it may be disclosed. The Attorney General must give the court a copy of the source document.
- **If the evidence is not in the form of a document** the Attorney General may allow a written summary of the information or a written statement of facts that the information would be likely to prove or a certificate stating the circumstances in which the information may be disclosed.

During the course of the trial the Attorney General's non-disclosure certificate is conclusive evidence that disclosure of the information is likely to prejudice national security.

Under section 31 the Act makes provision, following a voire dire, for the Court to order disclosure or partial disclosure in contravention of the Attorney General's certificate. If the Court does make those orders the Act requires the Court to adjourn the proceedings to allow any of the parties to appeal.

Jill Hill

10 August 2005

This paper is based on ALRC discussion paper 67.