Admission of evidence obtained in breach of privacy laws

By Liam Byrne

Photo © Dreamstime.com

This article examines the law relating to admissibility in Australian trials of relevant evidence obtained in breach of privacy laws, such as unauthorised telephone intercepts and evidence from unauthorised surveillance operations.

This issue is one aspect of the broader question of relevant but illegally obtained evidence, for which general rules have been developed by courts and legislatures. Commonwealth legislation has modified the common-law position relating to evidence obtained through telecommunications intercepts.[1] In some states, the general common-law rules otherwise apply, whereas in others, further legislation has modified the position for evidence obtained in breach of specific privacy laws. After first considering the broad principles involved, this article reviews the legislative approaches adopted in the Australian jurisdictions to the admissibility of unlawfully obtained evidence in general, and then the specific provisions relating to evidence obtained in breach of various privacy laws.

GENERAL PRINCIPLES

Courts deciding whether to exclude relevant but unlawfully obtained evidence are faced with two conflicting considerations. Excluding it may result in trials being decided without the most reliable and relevant evidence. Admitting it may be seen as legitimising illicit investigation methods.

The position adopted by the English (and Canadian) courts[2] prioritises the former consideration. The courts are not bound to exclude such information from criminal or >>

Excluding unlawfully obtained evidence may deny trials the most reliable and relevant evidence. Admitting it may be seen as legitimising illicit investigation methods.

civil trials. While English courts retain, in criminal trials, the usual discretion to exclude evidence because of unfairness or because its probative value is outweighed by its prejudicial effect, they do not appear to have a general discretion to exclude relevant information on the basis of illegality alone.[3]

The federal courts and legislature in the US have taken the opposite position. Evidence obtained unlawfully or though an unauthorised search[4] is generally excluded.

Courts in Australia, (and Scotland and Ireland),[5] on the other hand, have recognised (in criminal trials at least) a need to balance both of the principles when considering unlawfully obtained evidence. In the words of Barwick CJ in *R v Ireland*:

> 'whenever such unlawfulness or unfairness appears, the judge has a discretion to reject the evidence. He must consider its exercise. In the exercise of it, the competing public requirements must be considered and weighed against each other. On the one hand there is the public need to bring to conviction those who commit criminal offences. On the other hand is the public interest in the protection of the individual from unlawful and unfair treatment. Convictions obtained by the aid of unlawful or unfair acts may be obtained at too high a price. Hence the judicial discretion.'[6]

This discretion is unlike that exercised by the English courts because there is no requirement that the particular evidence be prejudicial, unfair or unreliable. The unfairness or unlawfulness of its manner of collection is the relevant consideration.

COMMON LAW

The Australian common-law position is as follows.

Authorities such as *Bunning v Cross* establish that, in criminal trials at least, the court must exercise the discretion described above when faced with unlawfully obtained evidence. Five factors to be considered in the exercise of that discretion were identified by Aickin and Stephen JJ in *Bunning v Cross*:

(a) whether the unlawfulness was deliberate (in which case the evidence is more likely to be excluded) or based on mistake;
(b) whether the unlawfulness affects the cogency of the evidence obtained;
(c) the ease with which the law could have been complied with in obtaining the evidence;
(d) the seriousness of the offence alleged against the defendant; and
(e) whether the legislation that made the method of obtaining the evidence unlawful suggests a deliberate parliamentary intent to restrict that method.

The unlawfulness that gives rise to the *Bunning v Cross* discretion may arise from breaches of statute or general law. While there is no common-law right to privacy in Australia, unlawfulness may arise where evidence is obtained as a consequence of a tort that strikes at a person's privacy. The most obvious example is unauthorised search and seizure amounting to trespass. While the courts have recognised an equitable jurisdiction to grant injunctions against disclosure of confidential documents and communications,[7] it is less clear that evidence obtained, particularly by an innocent third party, as a result of such disclosure would invoke the discretion.

While *Bunning v Cross*, like most of the authorities in this area, involved a criminal proceeding, the same public interests apply in civil trials. Accordingly, it seems that a court could, in appropriate circumstances, exercise a similar discretion in a civil proceeding. Of course, in both civil and criminal trials, other exclusionary rules and discretions continue to apply, even if evidence is not excluded by exercise of the *Bunning v Cross* discretion.

STATUTE

The common-law position has been modified by legislation in the Australian jurisdictions in three relevant ways.

Firstly, in some states and in the federal jurisdiction, the common law in relation to illegally obtained evidence has been modified by the terms of the Evidence Acts applying in those states.

Secondly, all Australian jurisdictions have introduced privacy legislation prohibiting certain types of surveillance, making evidence obtained in breach of such legislation unlawful and triggering the application of the rules on admissibility of unlawfully obtained evidence. On the other hand, legislation in each jurisdiction also expressly makes such surveillance lawful in certain circumstances.

Finally, in some states, specific statutory provisions directly modify the position in relation to evidence in breach of certain privacy laws.

Modification of the general common law

The Evidence Acts in force in the Commonwealth,[8] NSW and Tasmania have effectively replaced the common-law rules described above with a statutory regime. The statutes require courts faced with illegally obtained information to exercise a discretion similar to that described in *Bunning v Cross*. Significantly, though, the discretion is to be applied in both criminal and civil matters (whereas *Bunning v Cross* applies only to criminal matters).

The Evidence Acts in these jurisdictions all require the courts, in exercising the discretion, to consider various factors (set out in s138(3) of each Act):

(a) the probative value of the evidence and its importance in the proceeding;

(b) the nature of the offence, cause of action or defence, and the subject matter of the proceeding;
(c) the gravity of the impropriety or contravention, whether it was deliberate or reckless, and whether it was inconsistent with rights recognised by the *International Covenant on Civil and Political Rights* (ICCPR);
(d) whether any other proceedings (whether or not in a court) have been or are likely to be taken in relation to the impropriety or contravention; and
(e) the difficulty (if any) of obtaining the evidence without impropriety or contravening an Australian law.

The factors cover similar ground (albeit expressed differently) to those set out in *Bunning v Cross*. However, under the Acts, there is no requirement to consider the terms of the statute rendering the evidence-collection method unlawful and whether those terms indicate a deliberate legislative intent to prohibit the method by which the evidence was obtained. Nor is there a requirement to consider the effect of the unlawfulness on the cogency of the evidence (though its cogency will be considered under ss135 and 137). On the other hand, the Acts add a requirement to consider whether the unlawfulness is inconsistent with rights recognised by the ICCPR. Article 17.2 of the ICCPR includes a right to protection by law from arbitrary or unlawful interference with privacy. It might be arguable that, in the absence of a general right to privacy in Australian law, unlawfulness comprising a breach of the rights to protection against trespass or unauthorised listening or surveillance under Australian laws (which protect privacy-related interests) are rights recognised in Article 17.2.

Prohibition and authorisation of surveillance under privacy legislation

Commonwealth legislation prohibits the interception of communications passing over a telecommunications system, unless authorised under a warrant.[9] Legislation in each state and territory prohibits the use of listening devices to listen to or record private conversations unless authorised by statute or warrant.[10] Most states also prohibit or restrict unauthorised use of other surveillance devices,[11] such as cameras and other optical surveillance devices, data surveillance devices and tracking devices. Evidence obtained in breach of those provisions is 'unlawful' for the purposes of the rules described above. Furthermore, in some jurisdictions, specific rules apply to such evidence.

On the other hand, various pieces of Commonwealth, state and territory legislation authorise the use of surveillance devices or the interception of telecommunications, or provide for the issue of warrants authorising such use in specified circumstances.[12] Such authorisation renders the evidence obtained lawful (subject to any other illegality) and accordingly, pre-empts the operation of the discretion in *Bunning v Cross*, the relevant Evidence Act or the specific statutes described below.

Special rules on the admissibility of evidence in breach of privacy laws

Commonwealth

Section 77 of the Commonwealth *Telecommunications (Interception and Access) Act* 1979 renders evidence obtained from telecommunications intercepts inadmissible other than in certain prescribed circumstances. The prescribed circumstances provide for lawfully intercepted information (the lawfulness being determined on the balance of probabilities) to be given in evidence in an exempt proceeding.[13] Exempt proceedings are defined in s5B and cover 'serious offences' including murder, serious drug offences and offences punishable by a maximum penalty of imprisonment for life or in excess of seven years, among other things.[14]

States and territories

Legislation in NSW, Tasmania, Queensland and the ACT modifies the general rules as to admissibility of evidence obtained in breach of some of the privacy prohibitions described above.

Subject to certain exceptions, all of these laws make >>

While there is no common-law right to privacy in Australia, unlawfulness may arise where evidence is obtained as a consequence of a tort that strikes at a person's privacy.

certain evidence relating to unlawfully recorded private conversations inadmissible in criminal *and civil* trials, and remove the court's discretion[15] to admit it regardless.

The jurisdictions differ as to what evidence is affected. In Queensland, evidence of a conversation recorded in contravention of the relevant statute is excluded.[16] In the ACT, evidence of a conversation, including the production of a record of it, is caught.[17] In Tasmania and NSW, the net is cast broader, covering evidence of the conversation and other evidence obtained as a direct consequence of the conversation coming to the attention of a person in contravention of the relevant legislation.[18]

In NSW, Tasmania and the ACT, the unlawfully obtained evidence is *not* excluded in prosecutions for certain categories of serious crime specified in the respective Acts (generally including serious drug offences and other offences punishable by long prison terms).[19] However, its admission must still be determined by the exercise of the court's discretion under the general rule applying in the relevant state (that is, s138 of the relevant Evidence Act). In Queensland, on the other hand, under the corresponding provisions of the *Invasion of Privacy Act*, there is no exception permitting admission (on a discretionary basis) of unlawful telephone intercepts for serious offences.

Certain other exceptions also apply, including where:

(a) all (or, in Queensland, one of) the principal parties to the conversation all consent to admission of the evidence;[20]
(b) one of the principal parties to the conversation consented to its being recorded and the recording was reasonably necessary for the protection of the lawful interests of that party (provided that the party is not the state);[21]
(c) the call was inadvertently recorded or heard; and
(d) the defendant is being prosecuted for illegally recording the call.

The NSW Supreme Court has held that the prohibition in that state's *Listening Device Act* 1984 is inconsistent with the *Telecommunications (Interpretation and Access) Act* 1979 (Cth), and therefore that the state law no longer governs the admissibility of evidence obtained by telephone intercept.[22] The relevant provision is now s77 of the Commonwealth Act.[23]

CONCLUSIONS

The array of common-law and statutory provisions described above (see also the table set out below) means that the admissibility of the same evidence may be determined with different results from jurisdiction to jurisdiction. Different results can also arise depending on which privacy law is breached and what type of proceeding is in question.

For instance, evidence of a telephone conversation unlawfully recorded by use of a tape-recorder held near (but without the consent of) one of the parties to the

SOURCE OF APPLICABLE LAW ON ADMISSION OF ILLEGALLY OBTAINED INFORMATION

	Cth	NSW	Qld	SA	Tas	Vic	WA	ACT	NT
Evidence of unauthorised phone interceptions	*Telecommunications (Intercept and Access) Act* (Cth), s77 (applicable in all jurisdictions on the basis of *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222)								
Evidence of unauthorised conversation recordings	*Evidence Act*, s138	*Listening Devices Act*, s14	*Invasion of Privacy Act*, s46	Common law	*Listening Devices Act*, s10	Common law	Common law	*Listening Devices Act*, s14	Common law
Evidence obtained in breach of other privacy laws		*Evidence Act*, s138	Common law		*Evidence Act*, s138			*Evidence Act*, s138	
Other illegally obtained evidence									

call will be inadmissible in all civil proceedings in NSW, Queensland, Tasmania, and the ACT. In other states, the admission of such evidence in civil proceedings will be determined in accordance with the common law. In federal civil proceedings, the statutory discretion under s138 of the *Evidence Act* 1995 (Cth) will be applied.

If one considers admissibility of the same evidence in a serious criminal matter, though, the relevant statutory discretion will also apply in NSW, Tasmania and the ACT, and the common-law discretion in Queensland.

If the recording of the same conversation is intercepted as it passes over the telecommunications system, rather than being recorded by a tape recorder or other device external to the system, it will generally be inadmissible in civil matters in *all* jurisdictions, even where lawfully obtained.[24]

Accordingly, the most crucial steps in considering admissibility of evidence that may have been obtained in breach of a privacy law are:

(a) determining what privacy laws may have been breached;
(b) determining if any of the specific laws as to admission (that is, the *Telecommunications (Interception and Access) Act* 1979 (Cth), the *Listening Devices Act* 1984 (NSW), the *Invasion of Privacy Act* 1971 (Qld), the *Listening Devices Act* 1991 (Tas) or the *Listening Devices Act* 1992 (ACT)) apply, and applying them; and
(c) determining whether either the common law discretion or the discretion under the Commonwealth, NSW, Tasmania or ACT Evidence Acts applies and applying it. ■

Notes: **1** The term 'communications through a telecommunications' is defined in the *Telecommunications (Interception and Access) Act* 1979 to cover telephone messages but also the passing of messages in the form of data, music, images, etc, along a system for the carrying of communications by guided or unguided electromagnetic energy. **2** See *Bunning v Cross* (1978) 19 ALR 641 at 657. The general principles are also discussed at length in *Cross on Evidence* 7th Australian edition, J D Heydon, LexisNexis Butterworths, 2004. **3** *Bunning v Cross* (1978) 19 ALR 641 at 658 per Aickin and Stephen JJ, discussing *Kurama v R* [1955] AC 197 and *Jeffrey v Black* [1978] 1 All ER 555. **4** Unreasonable search and seizure is prohibited under the US Constitution. Evidence obtained from 'phone tapping', admitted by the Supreme Court in *Olmstead v US* 277 US 438 (1928), over dissenting judgments by Holmes and Brandeis, was subsequently prohibited by statute. **5** See *Bunning v Cross* (1978) 19 ALR 641 at 657. **6** (1970) 126 CLR 321 at 334, affirmed in *Bunning v Cross* (1978) 19 ALR 641. **7** For example, *Commonwealth of Australia v John Fairfax & Sons Ltd* (1980) 147 CLR 39. **8** The Commonwealth *Evidence Act* 1995 also applies in the ACT. **9** *Telecommunications (Interception and Access) Act* 1979 (Cth), s7. It has been held in *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222, that the Commonwealth Act covers the field with regard to telecommunications intercepts and, accordingly, the state Acts referred to in the next footnote do not apply to interception of telecommunications as such, although they may still operate – for example, where a listening device records speech after it has left the telecommunications system (such as a tape-recording of speech heard on a telephone handset). **10** *Listening Devices Act* 1984 (NSW), s5; *Invasion of Privacy Act* 1971 (Qld), s43; *Listening and Surveillance Devices Act* 1972 (SA), s4; *Listening Devices Act* 1991 (Tas), s5(1); *Surveillance Devices Act* 1999 (Vic), s6(1); *Surveillance Devices Act* 1998 (WA), section 5; *Listening Devices Act* 1992 (ACT), s4; *Surveillance Devices Act* 2000 (NT), s5. **11** For example, *Workplace Surveillance Act* 2005 (NSW), ss9, 15, 16, 19; *Surveillance Devices Act* 1999 (Vic), s6(1); *Surveillance Devices Act* 1998 (WA), s5; *Surveillance Devices Act* 2000 (NT), s5; *Listening and Surveillance Devices Act* 1972 (SA), s4. **12** For example, *Telecommunications (Interception and Access Act)* 1979 (Cth), chapter 2, part 2.2; *Surveillance Devices Act* 2004 (Cth), parts 2 and 3. **13** *Telecommunications (Interception and Access) Act* 1979 (Cth), s74. **14** *Telecommunications (Interception and Access) Act* 1979 (Cth), ss5, 5B, 5D. **15** Which would otherwise apply in Queensland to criminal trials under *Bunning v Cross*, and in all trials in the other jurisdictions under s138 of their respective Evidence Acts. **16** *Invasion of Privacy Act* 1971 (Qld), s46. **17** *Listening Devices Act* 1992 (ACT), s10. **18** *Listening Devices Act* 1984 (NSW), s13; *Listening Devices Act* 1991 (Tas), s14. **19** *Listening Devices Act* 1984 (NSW), s13(2)(d) (crimes carrying maximum prison terms of 20 years or more and certain specified drug offences); *Listening Devices Act* 1991 (Tas), s14(3)(d) (crimes carrying maximum prison terms of life or 21 years or more and certain specified drug offences); *Listening Devices Act* 1992 (ACT), ss10(2) and 3 (crimes carrying maximum prison terms of life or 10 years or more and certain specified drug offences). **20** *Listening Devices Act* 1984 (NSW), s13(2)(a); *Invasion of Privacy Act* 1971 (Qld), s46(2); *Listening Devices Act* 1991 (Tas), s13(3)(a); *Listening Devices Act* 1992 (ACT), s10(2)(a). **21** *Listening Devices Act* 1984 (NSW), s5(3)(b); *Listening Devices* Act 1992 (ACT), s10(2)(c). **22** Under s109 of the Constitution. **23** *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222. **24** Unless previously admitted in an 'exempt proceeding' (which includes certain serious criminal matters), in which case it may be admissible under s75A of the *Telecommunications (Interception and Access) Act* 1979 (Cth).

Liam Byrne *is a barrister at Selborne Chambers, Sydney.*
PHONE *(02) 9235 1155* **EMAIL** *liambyrne@selbornechambers.com.au*