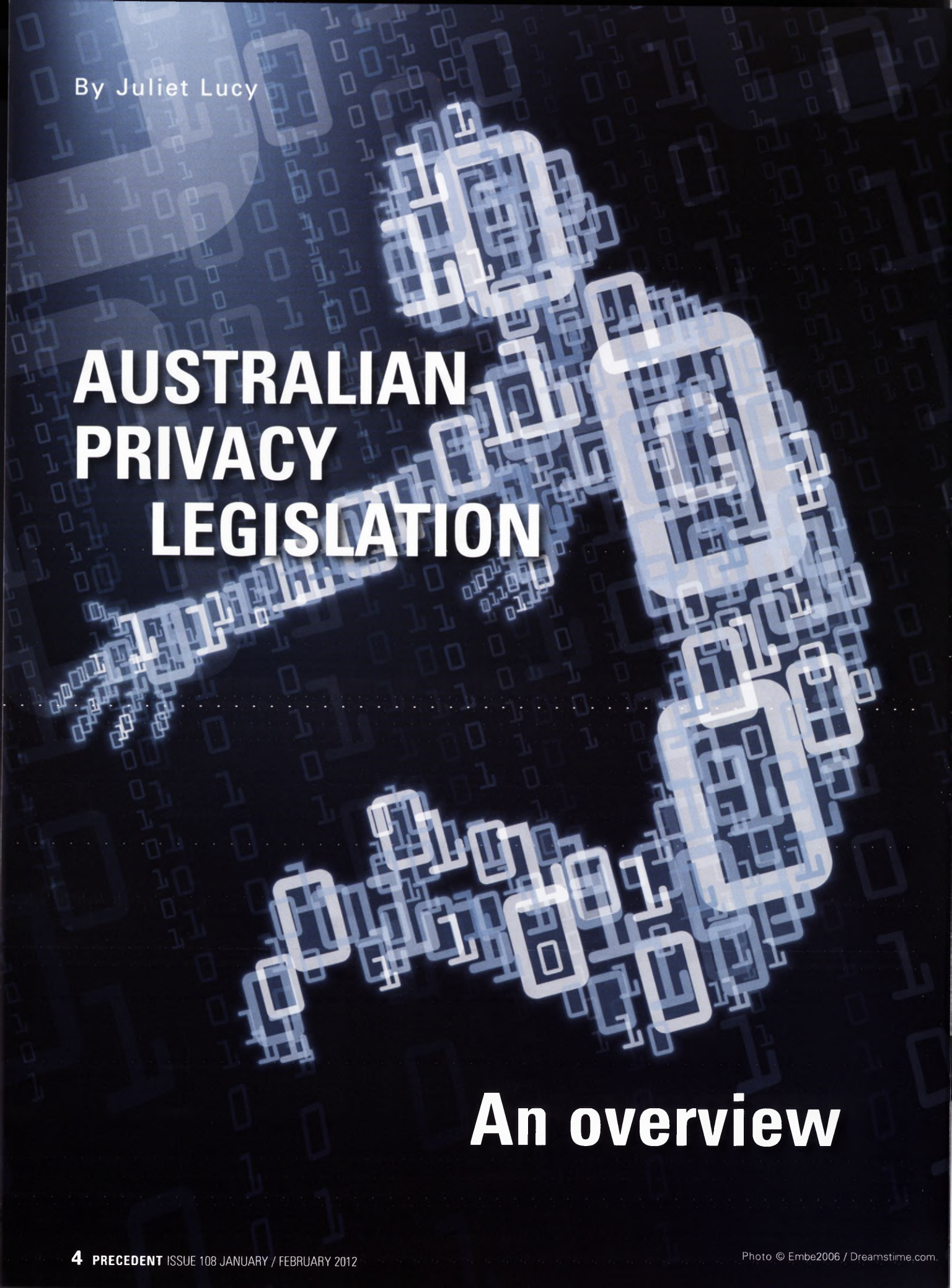
By Juliet Lucy

AUSTRALIAN PRIVACY LEGISLATION

An overview



The concept of a right to privacy was first recognised in international law after World War II, in Article 12 of the Universal Declaration of Human Rights (1946). It was subsequently recognised in a number of other international instruments.[1] The first significant step in developing principles to protect data, however, occurred in 1980 with the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which Australia adopted in 1984. The OECD Guidelines recognise general data protection principles, including a collection limitation principle, a data quality principle, a purpose specification principle, a use limitation principle and a security safeguards principle. These principles have formed the basis for Australian data protection laws.

The *Privacy Act* 1988 (Cth) was the first comprehensive data protection statute in Australia. Its Information Privacy Principles (IPPs) apply to Commonwealth government agencies handling information and regulate the collection, use and disclosure of personal information. Since 1994, they have been applied in a slightly amended version in the ACT.[2] In 2001, the application of the *Privacy Act* 1988 (Cth) was extended to the private sector by the inclusion of National Privacy Principles (NPPs). These cover the same general topics as the IPPs, as well as some additional topics, but differ in detail.

The following states and territories have also enacted data protection legislation (in order of enactment):

- ACT – *Health Records (Privacy and Access) Act* 1997 (ACT);
- New South Wales – *Privacy and Personal Information Protection Act* 1998 (NSW) and *Health Records and Information Privacy Act* 2002 (NSW);
- Victoria – *Information Privacy Act* 2000 (Vic) and *Health Records Act 2001* (Vic);
- Northern Territory – *Information Act* 2002 (NT);
- Tasmania – *Personal Information Protection Act* 2004 (Tas); and
- Queensland – *Information Privacy Act* 2009 (Qld).

South Australia has a non-legislative privacy scheme,[3] while Western Australia does not have any privacy legislation.

PRIVACY PRINCIPLES

Following the OECD model, Australian data protection legislation adopts privacy principles that are broad standards rather than prescriptive rules. The privacy principles regulate the collection, use and disclosure of personal and health information, as well as information security. Mostly, they apply to government agencies;[4] in some cases, to certain contracted service-providers;[5] and the Commonwealth NPPs and the health privacy principles in NSW, Victoria and the ACT apply to the private sector.[6]

'Personal information' is defined in the statutes, generally, as information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.[7] 'Health information' or 'personal health information' is generally a subset of 'personal information'.[8] While the privacy principles differ between jurisdictions, there are some broad similarities. An agency or, where applicable, an organisation, is generally prohibited from collecting personal or health information except where necessary for its functions or activities[9] and (except with the IPPs for the Commonwealth and Queensland and the health principles in the ACT) personal information must usually be collected from the individual to whom it relates.[10] That is, there is a prohibition against collecting personal or health information from third parties. There are also (except with the Commonwealth IPPs) requirements to inform the individual about certain matters when collecting personal or health information, such as the individual's access rights and the purposes of collecting the individual's information.[11]

The use of personal and health information is generally restricted to use for the purpose for which the information was collected, with specified exceptions allowing use for other purposes (such as with the individual's consent or with legal authorisation).[12] The record-keeper is also required to take reasonable steps to check the accuracy of the information before use.[13] There is a general prohibition against disclosure of personal or health information except for the collection purpose, with exceptions similar to those which apply to the use of personal and health information.[14]

An individual has a right to access his or her personal or health information[15] and the record-keeper may, in some circumstances, be required to amend that information on request to ensure its accuracy.[16] Finally, the record-keeper is required to ensure that personal and health information is protected, by taking >>

Photo © Dreamstime.com.

Broad standards rather than prescriptive rules, the Australian privacy principles apply mostly to government agencies and regulate the collection, use and disclosure of personal and health information, as well as information security.

reasonable security safeguards against misuse, loss and unauthorised access.[17]

COMPLAINTS AND REVIEW

There is a variety of processes for making complaints and redressing breaches of privacy in different jurisdictions. In many jurisdictions there is some kind of Commissioner, such as an Information Commissioner or Privacy Commissioner, who receives complaints and may mediate or conciliate them. In NSW, Victoria and Queensland, administrative tribunals play a role in reviewing or dealing with complaints.

Commonwealth

The Australian Information Commissioner encourages an individual to make his or her complaint about an alleged breach of a privacy principle first to the agency involved and to wait 30 days before making a complaint to the Commissioner.[18] When a person then makes a complaint to the Commissioner,[19] the Commissioner must generally investigate it if the conduct complained about may be an interference with the individual's privacy and, if appropriate, the Commissioner may endeavour to settle the matter by conciliation.[20] After investigating a complaint, the Commissioner may make a determination dismissing the complaint or find the complaint substantiated and make a determination accordingly.[21]

New South Wales

In the case of both personal and health information, an individual may apply for a review of an alleged breach of a privacy principle by the agency concerned; then, if the individual is dissatisfied with the outcome of the internal review, he or she may apply to the Administrative Decisions Tribunal (ADT) for a review of the conduct.[22] The ADT reviews the conduct said to be a breach of privacy afresh,[23] and there is a right of appeal on the law (and, with leave, on the merits) to the Appeal Panel of the ADT and, from the Appeal Panel's decision, on a question of law to the Supreme Court.[24]

An individual may also complain to the NSW Privacy Commissioner about a breach of his or her privacy by an agency.[25] The Privacy Commissioner may decide not to deal with the complaint if, for example, he or she is satisfied that it is frivolous, vexatious or lacking in substance.[26] If dealing with a complaint, the Privacy Commissioner must endeavour to resolve it by conciliation and may make a written report as to his or her findings or recommendations.[27] Complaints may also be made to the Privacy Commissioner about breaches of the health privacy principles by 'private sector persons' and complaints are dealt with by the Commissioner in a similar way to those about public sector agencies.[28]

Victoria

An individual may complain to the Victorian Privacy Commissioner about an act or practice that may be a breach of the privacy principles.[29] The Privacy Commissioner may decline certain complaints (such as those where the complainant has not first complained to the respondent or in the case of vexatious complaints).[30] The Privacy Commissioner may also conciliate a complaint.[31] If an agreement is reached through conciliation, the Commissioner may certify the agreement and a party may then register it with Victorian Civil and Administrative Tribunal (VCAT).[32] If a complaint is declined, or if conciliation fails, the complainant has a right to require the Privacy Commissioner to refer the complaint to VCAT for a hearing.[33]

Where health information is involved, an individual has a right to complain to the Health Services Commissioner about an alleged breach of the health privacy principles.[34] The Commissioner may decline the complaint in certain circumstances,[35] refer a complaint relating to a registered health service provider to the appropriate registration board where appropriate,[36] or accept the complaint. If he or she accepts the complaint, he or she may decide to conciliate the complaint, make a ruling or decline to further entertain the complaint.[37] A party may require the Commissioner to refer a ruling to VCAT.[38]

Queensland

An individual may complain to the Queensland Information Commissioner about an agency's

perceived failure to comply with the privacy principles 45 business days after making a complaint to the relevant agency.[39] The Information Commissioner may decline to deal with the complaint in certain circumstances, or may take reasonable steps to cause the complaint to be mediated.[40] If an agreement is reached through mediation, the Commissioner may certify it and a party may file the certified agreement with the Queensland Civil and Administrative Tribunal (QCAT).[41]

Tasmania

Complaints about breaches of the privacy principles in Tasmania are made to the Ombudsman.[42] The Ombudsman may decline to deal with the complaint, may refer it to another agency or may deal with it by conducting an investigation and advising the parties whether he or she is of the view that a privacy principle has been breached.[43]

Northern Territory

After requesting that a public sector organisation resolve the matter, an individual may complain to the Information Commissioner about a breach of his or her privacy.[44] The Commissioner must decide whether to accept or reject the complaint, and must investigate it if he or she accepts it.[45] If the Commissioner decides that there is sufficient *prima facie* evidence to substantiate the matter complained of, he or she must refer the matter to mediation.[46] If the mediation is successful, the parties may apply to the Commissioner to make orders giving effect to their agreement.[47] If it is not successful, the Commissioner must hold a hearing in relation to the complaint.[48] There is a right of appeal to the Supreme Court on a question of law from a decision of the Commissioner.[49]

ACT

Complaints concerning the IPPs or NPPs, as they apply in the ACT, are made under the *Privacy Act* 1988 (Cth).

A complaint concerning health information under the *Health Records (Privacy and Access) Act* 1997 (ACT) may be made to the ACT Human Rights Commission on the ground that an act or omission contravenes the privacy principles in relation to a consumer.[50] The Commission may refer a complaint for conciliation and, if a complaint is resolved by conciliation, it must help the parties to make a written record of the agreement they have reached.[51] Alternatively, the Commission may consider the complaint[52] (including, if it wishes, by exercising powers to require evidence to be provided), then close the complaint by making a written report.[53]

REMEDIES

Privacy is not always regarded as an area of the law with 'teeth'. This is perhaps because privacy principles have a certain flexibility to them and because the resolution of privacy disputes is often informal. However, in many jurisdictions, enforceable orders may be made that are similar to injunctions or to court orders to pay damages in personal injury cases. The difference is that the route to enforceability usually has more steps.

At Commonwealth level, the system involves first obtaining a declaration from the Australian Information Commissioner, then applying to a federal court to enforce it. If a complaint about a breach of the NPPs or IPPs is substantiated, the Commissioner may make a determination declaring that the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct; that the respondent should perform any reasonable act to redress any loss or damage suffered by the complainant; that the complainant is entitled to compensation for any loss or damage suffered; or that no further action should be taken.[54] While a declaration is not itself binding or conclusive, proceedings may be brought in the Federal Court or the Federal Magistrates Court for an order to enforce a determination relating to an organisation which is not an agency (that is, a private sector entity).[55] The court is to deal by way of a hearing *de novo* with the question whether the respondent has breached a privacy principle.[56]

Where the Australian Information Commissioner has declared that an agency must refrain from conduct or >>

Because an agency's or organisation's obligations with respect to data protection are not always clear, redressing breaches of privacy often involves considerable negotiation, medication or conciliation.

perform an act to redress any loss or damage suffered by the complainant, the agency must comply.[57] If it does not, the complainant may apply to the Federal Court or the Federal Magistrates Court for an order directing the agency to comply.[58] If the Privacy Commissioner declares that an agency must pay compensation, this becomes a debt due to the individual by the state or the agency.[59]

In NSW, Victoria and the Northern Territory, after reviewing an agency's conduct, the ADT, VCAT and the Northern Territory Information Commissioner respectively may make a range of orders, including an order requiring certain acts to be done or refrained from, and an order that the respondent pay compensatory damages of up to $40,000 (NSW), $100,000 (Vic) or $60,000 (NT).[60] In Victoria and Queensland, VCAT and QCAT may make orders giving effect to agreements reached through conciliation or mediation.[61]

FUZZY LAW?

Data protection remains an area of the law in which the scope of an agency's or organisation's obligations is not always clear cut, and in which the flexibility of the means for redressing breaches of privacy principles means that agencies, organisations and individuals often have to negotiate, mediate or conciliate to achieve outcomes. It is therefore not always easy to predict how an authority such as a commissioner or tribunal will evaluate an alleged breach of a privacy principle and, if a breach is established or agreed upon, what remedy will be achievable. Nevertheless, there is a growing body of law about what the privacy principles mean and the circumstances in which certain remedies will be appropriate. In NSW, in particular, there is a significant body of case law interpreting the privacy principles, principally consisting of ADT

decisions but also of Court of Appeal judgments.[62] This growing body of case law has made it easier to predict how the NSW privacy principles will be applied, making them more rule-like. There is also a substantial number of VCAT decisions, as well as decisions of the Queensland Information Commissioner, the former Federal Privacy Commissioner, the Australian Information Commissioner and the Federal Court, which provide guidance as to the application of the privacy principles in those jurisdictions.[63] ■

Notes: 1 *International Covenant on Civil and Political Rights*, Article 17 (opened for signature 1966, entered into force 1976); *European Convention for the Protection of Human Rights and Fundamental Freedoms*, Article 8 (opened for signature 1950, entered into force 1952). **2** *Australian Capital Territory Government Service (Consequential Provisions) Act* 1994 (Cth), s23, Sch. 3. **3** Government of South Australia Cabinet Administrative Instruction 1/89; also known as the Information Privacy Principles (IPPs) Instruction, and Premier and Cabinet Circular 12, as amended by Cabinet 18 May 2009 (hereafter, 'SA'). **4** *Privacy Act 1988* (Cth) (hereafter, 'Cth'), s16; *Privacy and Personal Information Protection Act* 1998 (NSW) (hereafter, 'NSW: P'), ss3, 20, *Health Records and Information Privacy Act* 2002 (NSW) (hereafter, 'NSW: H'), s4 (definition of 'organisation'), Sch. 1; *Information Privacy Act* 2000 (Vic) (hereafter, 'Vic: P'), s9(1), *Health Records Act* 2001 (Vic) (hereafter, 'Vic: H'), s10; *Information Act* 2002 (NT) (hereafter, 'NT'), s5(1); *Personal Information Protection Act* 2004 (Tas) (hereafter, 'Tas'), s17; *Information Privacy Act* 2009 (Qld) (hereafter, 'Qld'), s26; SA. **5** Vic: P, s9(1)(j), Vic: H, s12; NT, s5(7); Qld, s36. **6** Cth, s6C, Sch. 3, NSW: H, s11; Vic: H, s11; *Health Records (Privacy and Access) Act* 1997 (ACT) (hereafter, 'ACT: H'.) **7** Cth, s6; NSW: P, s4(1); Vic: P, s3; NT, s4; Tas, s3; Qld, s12; SA, cl. 3(1). **8** Cth, s6 (definition of 'health information', which is relevant for the NPPs); NSW: H, s6; ACT: H, Dictionary, definition of 'personal health information'; Vic: H, s3, definition of 'health information'. **9** Cth, ss14, IPP 1 and Sch. 3, NPP 1.1; NSW: P, ss8; NSW: H, Sch. 1, cl. 1(1); Vic: P, Sch. 1, cl. 1.1; Vic: H, Sch. 1, cl. 1.1; NT, Sch. 2, cl. 1.1; Tas, Sch. 1, cl. 1(1); Qld, Sch. 3, cl. 1 (IPP 1) and Sch. 4, cl. 1(1) (NPP 1(1)); ACT: H, Sch. 1, cl. 1(1). **10** Cth, Sch. 3, NPP 1.4; NSW: P, ss9; NSW: H, Sch. 1, cl. 3; Vic: P, Sch. 1, cl. 1.4; Vic: H, Sch. 1, cl. 1.3; NT, Sch. 2, cl. 1.4; Tas, Sch. 1, cl. 1(4); Qld, Sch. 4, cl. 1(4) (NPP 1(4)). **11** Cth, Sch. 3, NPP 1.3; NSW: P, ss10; NSW: H, Sch. 1, cl. 4; Vic: P, Sch. 1, cl. 1.3; Vic: H, Sch. 1, cl. 1.4, 1.5; NT, Sch. 2, cl. 1.3; Tas, Sch. 1, cl. 1(3); Qld, Sch. 3, cl. 2(3) (IPP 2(3)); Sch. 4, cl. 1(3) (NPP 1(3)). **12** Cth, ss14, IPP 11(1)(a), (c) and Sch. 3, NPP 2.1(b), (g); NSW: P, sss17(a), 25; NSW: H, Sch. 1, cl. 10(1)(a), (2); Vic: P, Sch. 1, cl. 2.1(b), (f); Vic: H, Sch. 1, cl. 2.1, 2.2; NT, Sch. 2, cl. 2.1(c), (f); Tas, Sch. 1, cl. 2(1)(b), (f); Qld , Sch. 3, cl. 10(1)(a), (c) (IPP 10) and Sch. 4, cl. 2(1)(b), (f) (NPP 2); ACT: H, Sch. 1, cl. 9(1)(a), (c). **13** Cth, ss14, IPP 8 and Sch. 3, NPP 3; NSW: P, ss16; NSW: H, Sch. 1, cl. 9; Vic: P, Sch. 1, cl. 3.1; Vic: H, Sch. 1, cl. 3.1; NT, Sch. 2, cl. 3.1; Tas, Sch. 1, cl.3; Qld, Sch. 3, cl. 8 (IPP 8) and Sch. 4, cl. 3 (NPP 3); ACT: H, Sch. 1, cl. 8. **14** Cth, ss14, IPP 11 and Sch. 3, NPP 2.1; NSW: P, ss18, 19; NSW: H, Sch. 1, cl. 11; Vic: P, Sch. 1, cl. 2.1; Vic: H, Sch. 1, cl. 2.2; NT, Sch. 2, cl. 2.1; Tas, Sch. 1, cl. 2(1); Qld, Sch. 3, cl. 11 (IPP 11); Sch. 4, cl. 2 (NPP 2); ACT: H, Sch. 1, cl. 10. **15** Cth, s14, IPP 6 and Sch. 3, NPP 6.1; NSW: P, s14; NSW: H, Sch. 1, cl. 7; Vic: P, Sch. 1, cl. 6.1; Vic: H, Sch. 1, cl. 6.1; NT, Sch. 2, cl. 6.1; Tas, Sch. 1, cl. 6(1); Qld, Sch. 3, cl. 6 (IPP 6); Sch. 4, cl. 6 (NPP 6); ACT: H, Sch. 1, cl. 5. **16** Cth, s14, IPP 7 and Sch. 3, NPP 6.5; NSW: P, s15; NSW: H, Sch. 1, cl. 8; Vic: P, Sch. 1, cl. 6.5; Vic: H, Sch. 1, cl. 6.5; NT, Sch. 2, cl. 6.3; Tas, Sch. 1, cl. 6(2); Qld, Sch. 3, cl. 7 (IPP 7); Sch. 4, cl. 7 (NPP 7); ACT: H, Sch. 1, cl. 7(2). **17** Cth, s14, IPP 4 and Sch. 3, NPP 4.1; NSW: P, s12(c); NSW: H, Sch. 1, cl. 5; Vic: P, Sch. 1, cl. 4.1; Vic: H, Sch. 1, cl. 4.1; NT, Sch. 2, cl. 4.1; Tas, Sch. 1, cl. 4(1); Qld, Sch. 3, cl. 2(3) (IPP 2(3)); Sch. 4, cl. 4(1) (NPP 4(1)); ACT: H, Sch. 1, cl. 4.1. **18** See http://www.privacy.gov.au/complaints/how and also Cth, s40(1A). **19** The right to make a complaint is conferred by s36(1) of the Cth Act. **20** Cth, ss27(1)(a), (ab), 40(1). **21** Cth, s52(1). **22** NSW: P, ss53(1), 55(1); NSW: H, s21. **23** *Administrative Decisions Tribunal Act 1997* (NSW), s63. **24** *Administrative Decisions Tribunal Act* 1997 (NSW), ss113, 119. **25** NSW: P, s45(1), (2); NSW: H, s21(1). **26** NSW: P, s46(3)(a). **27** NSW: P, ss48(1), 49(1), 50(1). **28** NSW: H, s42(1). **29** Vic: P, s25(1). **30** Vic: P, s29(1). **31** Vic: P, s33(1). **32** Vic: P, s35(1), (2). **33** Vic: P, ss29(5), (6), 37(3). **34** Vic: H, s45(1). **35** Vic: H, s51(1). **36** Vic: H, s52(1). **37** Vic: H, s56(1). **38** Vic: H, s65(1). **39** Qld, ss164, 165(1), 166(3). **40** Qld, ss168, 171(2). **41** Qld, ss172(4), 173(1). **42** Tas, s18(1), (2). **43** Tas, ss19-22. **44** NT, s104(1), (2). **45** NT, ss106(1), 110(1). **46** NT, s110(3), (4). **47** NT, s112(1). **48** NT, s113(1). **49** NT, s129(1). **50** ACT: H, s18(1)(a). **51** *Human Rights Commission Act* 2005 (ACT), ss51, 62(1). **52** *Ibid*, s52. **53** *Ibid*, Pt. 4, Div 4.4; ss78, 80. **54** Cth, s52(1)(b). **55** Cth, ss52(1B), 54(1), 55A(1). **56** Cth, s55A(5). **57** Cth, s58. **58** Cth, s62. **59** Cth, s60. **60** NSW: P, s55(2); NSW: H, s21; Vic: P, s43(1); NT, s115(1), (4). **61** Vic: P, s35(5); Qld, s173(2), (4). **62** The most significant Court of Appeal decisions are *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192 (agency not responsible for information held only in employee's mind) and *Director General, Department of Education and Training v MT* [2006] NSWCA 270 (agency's liability for unauthorised acts of employee). **63** These decisions are all available on Austlii.

Dr Juliet Lucy *is a senior solicitor at the NSW Crown Solicitor's Office. The views expressed in this article are not necessarily those of the Crown Solicitor.*

EMAIL *Juliet_lucy@agd.nsw.gov.au.*