

PRIVACY

LAW BULLETIN

Volume 4 Number 4

Print Post Approved 243459/00067

Information contained in this
newsletter is current as at
September 2007

Editorial board



Justice Michael Kirby
High Court of Australia

Kimberley Heitman
*Solicitor and Barrister, Director of
Legal Services UWA, Board Member of
Electronic Frontiers Australia*

Siobhan Jenner
*Legal and Policy Officer,
Privacy NSW*

Yee Fen Lim
*Senior Consultant,
Galaxia Consulting, Sydney*

Duncan Giles
Special Counsel, Freehills, Sydney

Catherine Parr
Partner, Allens Arthur Robinson

Katherine Sainty
Partner, Phillips Fox

Narelle Smythe
Partner, Clayton Utz

Blair Stewart
*Assistant Commissioner,
Office of the New Zealand
Privacy Commissioner*

Contents

Drawing the line between open justice and
personal privacy: New Zealand's tort of privacy
as applied in *Rogers v TVNZ*.....46

The NZ Court of Appeal recently decided on a case brought against a broadcaster for breach of privacy regarding a videotaped confession made by a criminally accused which was broadcasted following his acquittal. The decision highlights the steely approach taken in NZ to the defence of legitimate public concern and prior constraint issues.

Carolyn Heaton MORRISON KENT LAWYERS

ALRC calls for submissions on privacy discussion paper....50

The Australian Law Reform Commission recently released a discussion paper setting out 301 proposals for reform of the Australian privacy framework. This article sets out some of the key proposals by subject matter.

Kaman Tsoi and **Hannah Wright** FREEHILLS

The right to privacy in the Victorian Charter of Human
Rights and Responsibilities51

The Victorian *Charter of Human Rights and Responsibilities 2006* came into operation, in part, on 1 January 2007, with remaining provisions in effect from 1 January 2008. This article details the right to privacy aspects of the Charter.

Thaedra Frangos OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER

EYE SPY55

Privacy news in Australia and overseas



Drawing the line between open justice and personal privacy: New Zealand's tort of privacy as applied in *Rogers v TVNZ*

Carolyn Heaton
MORRISON KENT LAWYERS

The NZ Court of Appeal recently decided on a case brought against a broadcaster for breach of privacy regarding a videotaped confession made by an criminally accused which was broadcasted following his acquittal. The decision highlights the steely approach taken in NZ to the defence of legitimate public concern and prior constraint issues.

Murder in the Far North?

In September 1994, Katherine Sheffield's body was found in a shallow grave on the property of Borrie Lloyd in Mangonui, a Northland town four hours' drive from Auckland. Lloyd was charged with her murder. Subsequently, in 1995, Mr Lloyd was found not guilty of murder but guilty of manslaughter, and sentenced to 11 years' imprisonment.

On several occasions between 2001 and 2004, Noel Rogers, Mr Lloyd's nephew, was spoken to by the police about Mrs Sheffield's death. On 30 June 2004, he was arrested and charged with her murder.

While in prison on remand, Mr Rogers told his aunt, Mrs Lloyd, that he had killed Mrs Sheffield. She told the police that Mr Rogers wanted to return home and would assist the police with their enquiries if he was taken to Northland.

Despite a previous request from Mr Rogers' counsel not to have any communication with his client without

prior notification, two detectives arranged for Mr Rogers to be released into their custody for three days from 12 to 14 July 2004, so that he could be taken to Northland. On several occasions, Mr Rogers confirmed in writing that he had declined to have his lawyer present.

In the car on the way to the airport, one of the detectives received a call from Mr Rogers' counsel. When offered the phone, Mr Rogers declined to take it. At the place where Mrs Sheffield was killed, Mr Rogers was further advised of his rights and cautioned, and this was recorded on video. A reconstruction of the alleged crime was then filmed in which Mr Rogers gave an account of the manner in which he had killed Mrs Sheffield and disposed of her body.

In late July 2004, a copy of the reconstruction videotape was supplied to TVNZ by a police officer.

In August 2004, the NZ Court of Appeal quashed Mr Lloyd's conviction for manslaughter was quashed.¹

A preliminary hearing was then held, in February 2007, into the murder charge against Mr Rogers at which the reconstruction videotape was produced in evidence. Its admissibility was subsequently challenged and, at first instance, the NZ High Court ruled that the tape was admissible. On appeal, however, the Court of Appeal ruled that the confession and reconstruction evidence was inadmissible.²

On 7 February 2005, the Auckland High Court found Mr Rogers not guilty. The Crown case had been based on a number of admissions that Mr Rogers had made to other people, including his aunt. The defence argued that the admissions were based upon a dream that Mr Rogers had experienced and not on real events.

TVNZ intended to broadcast a current affairs program featuring the confession and reconstruction video on the Sunday following the acquittal. The trial judge heard an oral application on a *Pickwick* basis³ that day and ordered an interim injunction. On 15 February, the Full Court considered the matter afresh and permanently restrained TVNZ from broadcasting the videotape in whole or in part.⁴ The broadcaster was also ordered to deliver up to the court all copies of the videotape.

TVNZ appealed. The Court of Appeal was called upon to consider whether the tort of invasion of privacy had been made out, as its elements had been enunciated in *Hosking v Runting*,⁵ and whether there was any defence. Before continuing, it is necessary to first consider the context in which the stand-alone tort has been accepted in New Zealand.

Calling a spade a spade

In a 2005 article,⁶ Alexandra Sims referred to the 'stark choice' faced by NZ courts: either follow the English lead of applying an extended form of breach of confidence (leaving the traditional form of breach of confidence with its three elements⁷ 'unmolested'⁸), or reject that approach and continue with the development of the tort of invasion of privacy.

That choice was made by the Court of Appeal in *Hosking v Runting*,⁹ where the court said:

Once we dispense with any necessary link with obligations of confidence we prefer in the New Zealand legal environment to describe the cause of action as what it truly is.¹⁰

However, the development of a privacy tort has been 'continuing' since at least the interlocutory decision of Jeffries J in *Tucker v News Media Ownership Ltd*.¹¹ Here, in 1986, Mr Tucker needed to have a heart

transplant and was forced to mount a public drive to raise funds to allow him to travel to Australia for the surgery. News organisations found out about certain convictions he had for indecency going back some 10 years, and wanted to publish the details. Jeffries J granted injunctions against the news organisations on the basis of Mr Tucker's right to privacy, which the court recognised as a valid cause of action in NZ. Following appeal, the matter was referred by the Court of Appeal back to High Court for full trial. In the High Court, McGechan J held that common law was capable of adopting the principles laid out in *Wilkinson v Downton*¹² and extending the right to protect privacy.

Tucker has been considered, in subsequent High Court cases, to have created a tort of privacy.¹³ In *P v D*,¹⁴ another interim injunction decision,

an injunction restraining Pacific Magazines from publishing the photos, claiming intentional infliction of distress and invasion of their right to privacy.

The High Court decision was significant as the first outright rejection by a NZ Court of the tort of privacy. Randerson J also held that there had been no disclosure of private facts because the children were photographed in a public place. In an extensive look at the protection of privacy in other jurisdictions, Randerson J came to the conclusion that the High Court no longer recognised the tort of privacy, and that the extended form of breach of confidence should be used in future cases.¹⁵ However, at least one academic has suggested that Randerson J's discussion of the UK cases was descriptive rather than critically

Tucker has been considered, in subsequent High Court cases, to have created a tort of privacy.

Nicholson J set out (at 599) the four elements of the tort as being:

- a public disclosure;
- of private facts;
- that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities;
- without a legitimate public interest in disclosure.

Hosking v Runting

In this case, the Hoskings were 'celebrity' television personalities. Simon Runting was commissioned by the publisher of the *NewIdea* magazine to take some photographs of the Hoskings' two small children. The Hoskings had previously made public their IVF attempts, and after their subsequent separation there was a perceived public interest in the children. Without the knowledge or consent of the parents, Mr Runting took a photo of the two toddlers being pushed by their mother in a pushchair on a shopping street in Auckland. The Hoskings applied to the High Court for

analytical, and that the judge was being 'overly deferential'.¹⁶

When, in due course, the matter came before the Court of Appeal, three of the five judges¹⁷ held that a tort of invasion of privacy existed in NZ. However, the court did unanimously hold that NZ did not recognise a tortious cause of action in privacy based upon the publication of photos taken in a public place.

The tort, as formulated by Gault P and Blanchard J, comprised two limbs. First, '[t]he existence of facts in respect of which there is a reasonable expectation of privacy'; and second, '[p]ublicity given to those private facts that would be considered highly offensive to an objective reasonable person'.¹⁸ Tipping J proposed a less stringent test of 'substantial level of offence'.¹⁹

Although in *P v D* the absence of legitimate public interest was treated as an element of the tort itself, the court in *Hosking v Runting* stated that it was more conceptually sound for it to



constitute a defence, 'particularly given the parallels with breach of confidence claims, where public interest is an established defence'.²⁰

The court was also unanimous that it was not appropriate to use the extended form of breach of confidence in NZ, saying that '[p]rivacy and confidence are different concepts'.²¹ It was the majority's view that it was:

... legally preferable and better for society's understanding of what the Courts are doing to achieve the appropriate substantive outcome under a self-contained and stand-alone common law cause of action to be known as invasion of privacy'.²²

In essence, the court said:

... the developments in the United Kingdom, although via a different route, have arrived at a position not substantially different from the recognition of legal protection from publicity of private information. The New Zealand cases have not really gone beyond that.²³

In their minority judgments, Keith and Anderson JJ did not argue that privacy should not be protected, but that it is adequately and more carefully protected by means of the existing legislative framework and the common law actions available to safeguard privacy interests indirectly (for example, defamation, trespass, and copyright).

Despite the split in the Court of Appeal, and the fact that the court's acceptance of the breach of privacy tort was again obiter, it seems unlikely that there will be a fundamental shift in NZ's common law approach in the medium-term, particularly given the overlap between the judges on the bench for *Hosking v Runting* and the appointees to the new Supreme Court established in April 2004.

'No bright line?'²⁴

It is in this context, then, that three different NZ Court of Appeal judges²⁵ came to consider the facts in *Rogers v TVNZ*, to which I return.

Did the videotape contain facts in respect of which there was a reasonable expectation of privacy?

The primary fact contained in the reconstruction video was Mr Rogers' confession that he killed Mrs

Sheffield.²⁶ Was this a fact in respect of which there was a reasonable expectation of privacy in terms of the first limb of the tort?

The court was 'in no doubt' that although the circumstances at the time the facts came into existence would be relevant, this was to be assessed at the intended time of publication, not at the time when the tape was recorded (at [52]). It is the publicity given to the facts which gives rise to the interference, which is the gist of the tort.

Mr Rogers had an understanding and expectation when the videotape was recorded that its contents would be made public as part of the criminal process. However, although he had surrendered his privacy rights for the duration of the trial process, he had not surrendered them for all time. The court considered relevant that the videotape would normally have been in the safe keeping of the police until the trial, when it would have been under the control of the court. The court also noted that the tape was ruled inadmissible and that Mr Rogers was acquitted and was therefore innocent of murder (at [58]).

The court therefore found that there could be a reasonable expectation of privacy about the videotaped confession, even though it did not have an inherent quality of privacy. However, the privacy value to be attributed to the facts was 'at the low end of the scale' (at [59]), and this was important to the balancing exercise that had to be undertaken.

Would publication of the videotape be considered highly offensive to an objective, reasonable person?

The court was clear that what was to be considered was what a reasonable person with ordinary sensibilities would feel if placed in the same position as the claimant and faced with the same publication.²⁷

The court found no basis upon which to disagree with the High Court's view that it was highly offensive to contemplate disclosure of material obtained in fundamental breach of Mr Rogers' rights, and that the outcome would be humiliating and distressful for him.

Was the defence of legitimate public concern available?

The Court of Appeal regarded this aspect as being at the heart of the case.

The High Court had been satisfied that Mr Rogers' privacy right must prevail. It was not persuaded that use of the videotape in a current affairs program would in any way add to public debate and scrutiny of court processes. The admissibility decisions in the High Court and Court of Appeal had been fully reasoned, and use of the videotape would not add to a public understanding of the different decisions.

The Court of Appeal, on the other hand, considered that the defence of legitimate public concern was available, and that it was a matter of proportionality. The court said: 'the greater the invasion of privacy the greater must be the level of public concern to amount to a defence.'²⁸

Although there was 'some substance in the Full Court's view that the content of the videotape may not add to informed public debate', the court should nevertheless 'be prepared to expose its reasoning processes to scrutiny' in order to avoid any suggestion of an attempt to stifle debate about its decisions or about the actions of the police officers whose conduct was under scrutiny in those decisions (at [88]). Interestingly, William Young P indirectly acknowledged the power of the television medium by saying that: 'experience shows that arguments are usually more easily understood where they are contextualised' and that '[a]n esoteric argument about the way the New Zealand *Bill of Rights Act 1990* is applied by the Courts becomes far more accessible to the public if the implications can be assessed by reference to the concrete facts of a particular case' (at [128]).

Although Mr Rogers had a significant claim to privacy in relation to the videotape, the court was 'unpersuaded by some margin' that such claim should prevail over open justice considerations (at [89]), and cited with approval what Cory J said in *Vickery v Nova Scotia (Prothonotary of the Supreme Court)*²⁹ for the minority:

The public has a right to know what was excluded by the appellate court and the reason for its exclusion. To prohibit

access to all evidence which has been ruled inadmissible would permit the courts to operate in secret.

Prior restraint and the right to publish

While the courts have an acknowledged jurisdiction to restrain the publication of material, the importance placed upon freedom of expression means that it has been called ‘a wholly exceptional jurisdiction to be exercised only in cases where there is a well-grounded fear that the publication will be clearly unlawful’ and that ‘it is not part of the function of the Court to act as censor’.³⁰

In respect of prior restraint, the Court of Appeal in *Runting v Hosking* said:

The general position, then, is that usually an injunction to restrain publication in the face of an alleged interference with privacy will only be available where there is compelling evidence of most highly offensive intended publicising of private information and there is little legitimate public concern in the information. In most cases, damages will be considered an adequate remedy.³¹

In his judgment, William Young P said that the Full Court’s conclusion that TVNZ’s planned current affairs program could not serve the public interest was ‘extremely bold, indeed far too bold given orthodox prior restraint principles’ (at [130]).

Although the disclosure in *Rogers* met the ‘highly offensive’ threshold, it was not ‘at the high end of highly offensive’ (at [96]) and there was more than ‘little legitimate public concern’.³²

Referring to *WB and H Bauer Publishing Ltd*,³³ and the fact that Mr Rogers could have a claim in defamation if TVNZ screened a program impugning his acquittal, the court confirmed the wisdom of a consistent prior restraint test for both defamation and privacy.

Comment

It is interesting to consider that Mr Rogers’ claim may have had a greater chance of success if it had been considered in England. Given the obscurity that surrounded TVNZ’s receipt from the police of the videotape well before Mr Rogers’ trial, the extended breach of confidence action

could be applied, using Lord Woolf’s ‘reasonable expectation of privacy’ test from *A v B plc*.³⁴

A duty of confidence will arise whenever the party subject to the duty is in a situation where he either knows or ought to know that the other person can reasonably expect his privacy to be protected.

The NZ Court of Appeal, although prepared to find a breach of Mr Rogers’ privacy in terms of the two limbs of the tort, nevertheless demonstrated a steely approach to the defence of legitimate public concern and to prior restraint issues, indicating that it is not going to be easy for NZ claimants to tip the balance away from freedom of expression. ●

Carolyn Heaton, Morrison Kent Lawyers, Wellington, New Zealand.

Endnotes

1. *R v Lloyd* (Court of Appeal, CA 72/02, 25 August 2004).
2. *R v Rogers* [2006] 2 NZLR 156.
3. This is the practice of serving copies of an ex parte application on the opposing party at the same time as it is filed in court, enabling the defendant to be heard and avoiding the need for further proceedings at a later date to set the injunction aside; from *Pickwick International Inc (GB) Ltd v Multiple Sound Distributors Ltd* [1972] 3 All ER 384.
4. Unreported, High Court, Auckland, CIV2005-404-7152, 22 December 2005, Venning and Winkelmann JJ.
5. [2005] 1 NZLR 1.
6. Sims A “‘A shift in the centre of gravity’”: the dangers of protecting privacy through a breach of confidence” (2005) *Intellectual Property Quarterly* 27–51.
7. In *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, Megarry J set out the elements of breach of confidence as follows:

First, the information itself ... must have the necessary quality of confidence about it. Secondly, that information must be imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.

8. Above note 5. The *Coco* formulation of breach of confidence is to be compared to the extended form of the action used to protect privacy in England. For more on this, see Carey S ‘Obiterated! Should New Zealand follow the United Kingdom’s lead in extending breach of confidence to cover privacy?’ (2005) *New Zealand Post Graduate Law E-journal* issue 1, article 5.

9. Above note 4.
10. See above note 4 at [110].
11. Unreported, High Court, Wellington, CP477/86, 22 October 1986.
12. [1897] 2 QB 57.
13. Including *Bradley v Wingnut* [1993] 1 NZLR 415.
14. [2000] 2 NZLR 591.
15. [2003] 3 NZLR 385, at [419], [420].
16. Carey, above note 7.
17. Gault P, Blanchard and Tipping JJ; Keith and Anderson JJ dissenting.
18. Above note 4 at [117].
19. Above at [256].
20. Above at [129].
21. At [48].
22. See above note 4 at [246] (Tipping J).
23. See above note 4 at [90] (Gault P and Blanchard J).
24. This refers to the phrase used by Gleeson CJ in *ABC v Lenah Game Meats Pty* (2001) 208 CLR 199 to describe the difficulty inherent in determining what is private and what is not. I use the phrase here also to refer to the line to be drawn between open justice and personal privacy.
25. William Young P, O’Regan and Pankhurst JJ.
26. [2007] 1 NZLR 156 at [48].
27. At [66] referring to *Campbell v MGN Limited* [2004] 2 AC 457 per Lord Hope of Craighead (at [99]).
28. Above note 26 at [86], citing Tipping J in *Hosking v Runting* (at [257]).
29. [1991] 1 SCR 671 at 706.
30. *Auckland Area Health Board v TVNZ* [1992] 3 NZLR 406 at 507 (NZ Court of Appeal).
31. At [158].
32. See above note 20 and the accompanying text.
33. [2002] EMLR 8. This case concerned the admissibility of a DNA sample and publication of the name of the defendant acquitted of rape.
34. [2002] 3 WLR 542.



ALRC calls for submissions on privacy discussion paper

Kaman Tsoi and Hannah Wright FREEHILLS

On 12 September 2007, the Australian Law Reform Commission (ALRC) released a significant discussion paper entitled *Review of Australian Privacy Law*. The discussion paper forms part of an ALRC review, initiated by the federal government, of Australia's privacy framework. The final report of the ALRC is due to the government by 31 March 2008.

The review was established primarily in response to:

- rapid advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which privacy should be protected by legislation;
- the expansion of state and territory legislative activity in areas relevant to privacy; and
- emerging areas that may require privacy protection generally.

The latest discussion paper sets out over 300 proposals for reform of the Australian privacy framework, as well as asking many questions in connection with the ALRC's inquiry generally.

This article sets out some of the key proposals of the ALRC by subject matter. Further, detailed analysis of the proposals will be covered in the next issue of the *Privacy Law Bulletin*.

General

- Introduce one set of unified privacy principles, based on the current National Privacy Principles (NPPs), to apply to all private sector organisations and the federal public sector.
- Extend some privacy protections to the personal information of deceased persons.
- Require that the collection of information be relevant the purpose for which it is collected.

- Remove the small business exemption.
- Publish a list of overseas laws and schemes which provide similar protection to Australian privacy laws, facilitating transfer of information to those countries.
- Hold organisations liable for information sent to third parties overseas, in some circumstances.
- Require agencies and organisations to notify individuals when there has been a data breach and there is a real risk of serious harm.
- Empower the Privacy Commissioner to take court action to enforce its order requiring an agency or organisation to take some action within a specified timeframe.
- Empower the Privacy Commissioner to take court action in the event of serious or repeated contravention of the law.
- Develop a statutory cause of action for invasion of privacy.

Employment

- Remove the employee records exemption for private sector organisations.

Credit reporting

- Increase in the information that can be included in a credit reporting file to include:
 - type of each current credit account opened;
 - date of opening of the current credit account;
 - limits on each current credit account; and
 - date of closure of current credit account.
- Require credit providers to be members of an external dispute resolution scheme before they can provide default information to a credit reporting agency.

- Remove a default listing from a credit report if a dispute in relation to that listing is not addressed within 30 days.
- Enable individuals to notify credit reporting agencies of identity theft so that the identity theft can be reported to potential credit providers.

Health

- Introduce one set of new health regulations to override state and territory health privacy laws as they apply to the private sector.
- Encourage states and territories to adopt new health privacy principles for their public sectors.
- Develop specific legislation for the regulation of an electronic health record scheme, including the treatment of unique healthcare identifiers.
- Enable healthcare providers to collect third-party personal information without that third party's consent, if relevant and necessary.
- Introduce procedures for the closure of a health service or transferring of a health service to a new owner.

Marketing

- Introduce a separate privacy principle addressing direct marketing in the private (and possibly public) sector. Such a principle would require:
 - consent, unless it is impracticable to gain consent;
 - express consent for sensitive information; and
 - a clearly set out opt-out regime.

Technology and telecommunications

- Ensure privacy laws are technologically neutral, but allow the Privacy Commissioner to develop guidelines on how to apply the *Privacy Act 1988* (Cth) to particular forms of technology.
- Consider introducing a 'take down notice' scheme requiring a

website operator to remove information that might be an invasion of an individual's privacy.

- Prohibit charging for unlisted phone numbers.
- Include email addresses and IP addresses in the definition of 'personal information'.

Government

- Apply rules relating to transborder data transfer, anonymity and sensitive information to the federal public sector.
- Encourage states and territories encouraged to adopt new unified privacy principles for their public sectors.
- Remove the political exemption.

The deadline for feedback on these and other issues raised in the discussion paper is 7 December 2007. For further information, visit <www.alrc.gov.au>. ●

Kaman Tsoi, Senior Associate, and Hannah Wright, Solicitor, Freehills, Melbourne.

The right to privacy in the Victorian Charter of Human Rights and Responsibilities

Thaedra Frangos

OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER

The Victorian *Charter of Human Rights and Responsibilities Act 2006* (the Charter) came into operation, in part, on 1 January 2007. The remaining Divisions will take effect from 1 January 2008. The Charter applies to public authorities.¹

The ACT is currently the only other Australian jurisdiction with human rights legislation.² Both WA and Tasmania are considering Bill of Rights legislation,³ and there have been several attempts at similar legislation at a Commonwealth level.⁴ Canada, the US and South Africa have Bills of Rights contained in their constitutions, while the UK and NZ have human rights legislation.

Compatibility of legislation with the Charter

Since the Charter commenced, new legislation introduced into the Victorian Parliament must be accompanied by a statement of compatibility with the human rights protected by the Charter.⁵ This statement must precede the Second Reading speech and state, in the opinion of the relevant Member of Parliament, whether the Bill is compatible with human rights and, if so, how it is compatible. If any part of the Bill is considered to be incompatible

with the Charter, the statement must set out the nature and extent of the incompatibility. Statements of compatibility are not binding on any court or tribunal⁶ and failure to issue a statement of compatibility for a Bill that becomes an Act will not affect the Act's validity, operation or enforcement.⁷ In practice, statements of compatibility are generally prepared as part of the Cabinet process by policy and legislative officers in the relevant department.

From 1 January 2008, the Charter will provide for statutory provisions to be interpreted, as far as is possible, in a way that is compatible with human rights and, for the referral, in particular circumstances, of questions of law and, questions of interpretation of statutory provisions in accordance with the Charter, to the Supreme Court.⁹ The Supreme Court will be empowered to make a declaration that a provision cannot be interpreted consistently with the Charter. This declaration will not

Since the Charter commenced, new legislation introduced into the Victorian Parliament must be accompanied by a statement of compatibility with the human rights protected by the Charter.

The Charter contains an override provision whereby Parliament may declare that an Act or provision, and any relevant subordinate instrument made under that Act, is effective despite being incompatible with one or more of the Charter rights. It is intended that this section operate only in exceptional circumstances (for example, threats to national security).⁸

affect the validity of the relevant provision, however it will require the relevant Minister to table in Parliament, his or her response to the declaration.¹⁰ Further, the Charter imposes an obligation on public authorities to give appropriate consideration to human rights in their decision making as well as making it unlawful, in most circumstances,¹¹ for a public authority



to act in a way that is incompatible with a human right.¹²

Right to privacy

The Charter contains a right to privacy based on art 17 of the International Covenant on Civil and Political Rights. The right also mirrors the right to privacy and reputation in the ACT legislation.¹³ Section 13 of the Charter expresses the right to privacy as follows.

A person has the right —

- (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with;

...

privacy is also limited in itself to the extent that it allows for interference provided that interference is both lawful and not arbitrary.

The UN Human Rights Committee has useful comments on interference.¹⁸

- ‘The term “unlawful” means that no interference can take place except in cases envisaged by the law.

Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.’

- ‘The expression “arbitrary interference” is also relevant to the protection of the right provided for in article 17. In the Committee’s view

However, the Charter right to privacy is broader ... and may encompass bodily, territorial, communications and locational privacy, in addition to information privacy.

Privacy is not defined in the Charter and it is intended that the right be interpreted consistently with the *Information Privacy Act 2000* (Vic) (IPA) and the *Health Records Act 2001* (Vic),¹⁴ which regulate information privacy in Victoria. However, the Charter right to privacy is broader than the privacy protected by those Acts and may encompass bodily, territorial, communications and locational privacy, in addition to information privacy.

Limitations on the right to privacy

All Charter rights may be limited to the extent that the limitation is ‘demonstrably justified in a free and democratic society based on human dignity, equality and freedom’¹⁵ and by consideration of all relevant factors such as the nature of the right and the importance of the purpose for limiting the right. The nature of the right to privacy is that it is not an absolute right¹⁶ and will often need to be balanced with other rights, such as freedom of expression.¹⁷ The right to

the expression “arbitrary interference” can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.¹⁹

In the *Toonen* decision,²⁰ the Human Rights Committee also stated that reasonable interferences with privacy are those ‘based on reasonable and objective criteria and which are proportional to the purpose for which they are adopted’. In relation to ‘arbitrary’, it was considered that it ‘was meant to cover interferences which, under Australian law, would be covered by the concept of “unreasonableness”’. The Committee also regarded domestic social mores as relevant to the determination of whether a lawful interference with the right to privacy was also reasonable and not arbitrary.

In her Law Week address, the Victorian Privacy Commissioner pointed out that, due to s 6(1) of the IPA, which provides that in the event of inconsistency the IPA submits to other legislation, 'the right to privacy under the Charter is stronger than the IPA in that the fact that a breach of privacy is lawful does not mean that it will be compatible with the Charter unless it also passes the test of "reasonableness"'.²¹

Since the Charter came into operation in Victoria, the right to privacy has been referred to in the compatibility statements for a number of Bills including amendments to the *Crimes Act 1958* (Vic),²² sports betting legislation²³ and rules for admission to the legal profession.²⁴ The discussion of whether a provision is an arbitrary interference has centred around such factors as whether discretionary decision making is limited, circumscribed and precise in scope,²⁵ and if the provision effectively balances competing rights, such as freedom of expression, with the right to privacy.

The Victorian Parliament Scrutiny of Acts and Regulations Committee

Section 30 of the Charter extends the role of the Scrutiny of Acts and Regulations Committee (SARC) to require that it considers and reports on whether a Bill is incompatible with human rights. The Victorian Privacy Commissioner recently made a submission²⁶ to SARC in relation to the Justice and Road Legislation Amendment (Law Enforcement) Bill 2007 (Vic) on the basis that the proposed legislation:

- unduly required or authorised acts or practices that may have an adverse effect on personal privacy within the meaning of the IPA;²⁷ and
- was incompatible with the right to privacy in the Charter.²⁸

Thus, the expansion of SARC's role in the scrutiny of new legislation and regulations has also established a broader legislative basis upon which the Privacy Commissioner, in accordance with his or her functions,²⁹ may comment on the privacy impact of a particular Bill.

Cause of action for privacy under the Charter

While the Victorian Equal Opportunity and Human Rights Commission is empowered³⁰ to monitor, review and report on the operation of the Charter, there is no mechanism for individuals to complain to an independent agency about a breach of human rights by a public authority. Further, the Charter does not establish a discrete cause of action for individuals to seek relief or damages for breach of human rights.³¹ However, it does provide that where there is an existing cause of action outside of the Charter, unlawfulness as provided by s 38 of the Charter³² may constitute an additional ground for the action.

In relation to the right to privacy, Dr Simon Evans has suggested that the ability to add the ground of unlawfulness on the basis of the Charter to an existing cause of action could enable expansion of the type of conduct by public authorities that may trigger the court's discretion to exclude particular evidence where it has been obtained through unlawful conduct (for example, evidence obtained through unlawful surveillance).³³ In the absence of Victorian case law on this subject since the Charter came into operation,³⁴ the effect of this provision remains to be seen. Another significant issue for consideration in relation to causes of action for unlawfulness under the Charter is the development of a common law tort of privacy in Victoria following the case of *Jane Doe v ABC*.³⁵ The NSW Law Reform Commission³⁶ and the Australian Law Reform Commission are also currently considering this developing area of privacy law. ●

Thaedra Frangos, Manager, Policy, Office of the Victorian Privacy Commissioner.

Endnotes

1. For the definition of 'public authority', see s 4.
2. *Human Rights Act 2004* (ACT).
3. In May 2006, the WA Attorney-General, Jim McGinty, signalled an intention to develop a Bill of Rights: see Chaney F 'WA starts human rights journey' *ABC Online* 7 May 2007;

available at <www.abc.net.au/news/opinion/items/200705/s1914502.htm>.

A draft WA *Human Rights Act* was released in May 2007, with submissions closing on 31 August 2007: see <www.humanrights.wa.gov.au>. The Tasmanian Law Reform Commission is currently considering submissions on its issues paper, *A Charter of Rights for Tasmania?* (Issues Paper No 11, released 31 August 2006); available at <www.law.utas.edu.au/reform/Projects/Human%20Rights.htm>.

4. Parliamentary Charter of Rights and Freedoms Bill 2001 (Cth). See also the opinion article from federal Attorney-General Phillip Ruddock 'Bill of Rights do not protect freedoms' *Sydney Morning Herald* 31 August 2007.

5. Section 28(3)(a) and (b).

6. Section 28(4).

7. Section 29.

8. See s 31(4) and the Explanatory Memorandum to the Charter Bill, at p 21.

9. Sections 32 and 33.

10. Sections 36 and 37 respectively.

11. Section 38(2) provides that s 38(1) does not apply if the authority is not reasonably able to act differently due to the requirements of another law.

12. Section 38.

13. *Human Rights Act 2004* (ACT), s 12.

14. Explanatory Memorandum to the Charter Bill at p 13.

15. Section 7(2).

16. Such as the right to life in s 9 of the Charter. Further, as contained in s 5(1) of the IPA, the intention of the Act is to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector.

17. Section 15.

18. Section 32(2) of the Charter provides that '[i]nternational law and the judgments of domestic, foreign and international courts and tribunals relevant to a human right may be considered in interpreting a statutory provision'.

19. General Comment No 16, paras 3 and 4.

20. Communication No 488/1992: Australia 04/04/94. This was a case



whereby a Tasmanian man challenged the validity of the Tasmanian *Criminal Code* which prohibited sexual contact between two males. The UN Human Rights Committee held that the legislation contravened art 17 of the International Covenant on Civil and Political Rights.

21. Versey H *Human Rights — the Privacy Balancing Act*, presentation for Law Week, Victoria University, 15 May 2007, p 11 available at www.privacy.vic.gov.au/dir100/priweb.nsf/content/F776BE46B0105C42CA256C4D0019BD50?OpenDocument.

22. *Crimes Amendment (DNA Database) Act 2007* (Vic).

23. *Gambling and Racing Legislation Amendment (Sports Betting) Act 2007* (Vic).

24. *Legal Profession Amendment (Education) Bill 2007* (Vic).

25. See, for example, Parliament of Victoria, Statement of Compatibility of the Accident Towing Services Bill *Hansard* 19 April 2007 at p 1146.

26. See Victoria Scrutiny of Acts and Regulations Committee *Alert Digest No 10 of 2007* (7 August 2007), available at www.parliament.vic.gov.au/sarc/Alert_Digests_07/07alt10body.htm#Justice_and_Road_Legislation_Amendment_Law_Enforcement_Bill_2007.

27. *Parliamentary Committees Act 2003* (Vic), s 17(a)(iv).

28. Above, s 17(a)(viii).

29. *Information Privacy Act 2000* (Vic), s 58(l).

30. Part 4 of the Charter.

31. The Explanatory Memorandum to the Charter Bill (p 27) refers to Parliament's intention that the Charter 'does not create any independent cause of action or any independent forms of relief'. See also s 39 of the Charter.

32. Section 38(1) provides:

Subject to this section, it is unlawful for a public authority to act in a way that is incompatible with a human right, or in making a decision, to fail to give proper consideration to a relevant human right.

33. Evans S 'The Victorian Charter of Rights and Responsibilities and the ACT Human Rights Act: four key differences and their implications for Victoria', paper presented to *Australian Bills of Rights: The ACT and Beyond Conference*, Australian National University, 21 June 2006, p 12.

34. In the Victorian Court of Appeal decision in *Royal Women's Hospital v Medical Practitioners Board of Victoria* [2006] VSCA 85; BC200602419, which was handed down prior to the Charter's coming into operation, Maxwell P stated (at [72]) that 'there is a proper place for human rights-based arguments in Australian law cannot be doubted' and emphasised the following:

1. The Court will encourage practitioners to develop human rights-based arguments where relevant to a question in the proceeding.
2. Practitioners should be alert to the availability of such arguments, and should not be hesitant to advance them where relevant.
3. Since the development of an Australian jurisprudence drawing on international human rights law is in its early stages, further progress will necessarily involve judges and practitioners working together to develop a common expertise.

For further commentary on this case, see Victorian Government Solicitors Office 'Right to Privacy enhanced by the Charter' *Charter of Human Rights Newsletter* at pp 4–5, available at www.vgso.vic.gov.au/resources/Temp/HRC4.pdf.

35. [2007] VCC 281 (the ABC has appealed this County Court decision). For a discussion of this case in the *Privacy Law Bulletin*, see Wilson T 'Victim's details protected — a new privacy right? Jane Doe v ABC, Rickard and Veo' (2007) 3(10) *Priv LB* 126 and Ryan I 'Has privacy gone too far? Doe v ABC and its potential impact on journalism' (2007) 4(1) *Priv LB* 7. See also Wright F 'The Jane Doe Case' (Autumn 2007) Vol 6 No 1 *Office of the Victorian Privacy Commissioner Privacy Aware Newsletter* p 3, available at: www.privacy.vic.gov.au/dir100/priweb.nsf/content/3D4B3085A784AEA9CA256C5A0081E819?OpenDocument.

36. For further information on the ALRC review see www.austlii.edu.au/au/other/alrc/publications/issues/31/. The NSW LRC Review is discussed in Wilson T 'Privacy law recommended in NSW' (2007) 4(3) *Priv LB* 38. Details on this review are available at www.lawlink.nsw.gov.au/lawlink/lrc/lrc.nsf/pages/LRC_cref113.

eye spy PRIVACY NEWS

Australia

ALRC releases privacy discussion paper

12 September 2007. The Australian Law Reform Commission (ALRC) has released a blueprint with 301 proposals for overhauling Australia’s privacy laws and practices.

ALRC President Professor David Weisbrot said that the discussion paper, *Review of Australian Privacy Law*, was the product of the largest public consultation in ALRC history.

‘The ALRC is proposing there be a single set of privacy principles for information-handling across all sectors, and all levels of government,’ said Weisbrot. ‘This will make it easier and less expensive for organisations to comply, and much more simple for people to understand their rights.’

‘The protection of personal information stored or processed overseas, as is now routine, is another serious concern. The ALRC wants to ensure that such information has at least the same level of protection as is provided domestically. We propose that a government agency or company that transfers personal information overseas without consent should remain accountable for any breach of privacy that occurs as a result of the transfer.’

Commissioner in charge of the inquiry, Professor Les McCrimmon, said that the ALRC also is proposing a new system of data breach notification.

‘There is currently no requirement to notify individuals when there has been unauthorised access to their information, such as when lists of credit card details are inadvertently published. Where there is a real risk of serious harm to individuals, we say they must be notified,’ said McCrimmon.

Submissions close on 7 December 2007 and copies of the discussion paper are available at <www.alrc.gov.au>.

An overview of the key proposals appear on p 50 of this issue of the

Privacy Law Bulletin. Further detailed discussion will appear in the October issue. ●

Source: ALRC media release (12 September 2007).

APEC ministers endorse data privacy initiative

6 September 2007. APEC ministers have endorsed the APEC Data Privacy Pathfinder initiative, which will result in the establishment of an effective system for protecting an individual’s personal information throughout the Asia-Pacific region.

The Pathfinder initiative involves a group of APEC economies developing and road-testing a range of practical projects. The projects include:

- providing business with guidance on developing cross-border privacy rules;
- encouraging the development of cooperative and information-sharing arrangements between regulators in different economies; and
- exploring the role of private sector ‘trustmarks’ to check business privacy policies and assist in resolving customer complaints. ●

Source: Federal Attorney-General Philip Ruddock media release 194/2007 (6 September 2007).

Government sets up taskforce on social networking websites

13 September 2007. The federal government has announced terms of reference for the consultative working group to address the potential serious abuse of social networking sites by paedophiles and sex offenders to contact and groom children.

The working group will report on the nature and scope of the criminal threat posed by social networking sites for grooming children for sexual offences. It will report on existing measures and suggest reforms that could assist in providing children with more protection when they use these sites.

The initiative is an extension of the

government’s \$189 million *NetAlert* — *Protecting Australian Families Online* program. ●

Victoria latest to enable matching of data on DNA databases

25 July 2007. The *Crimes Amendment (DNA Database) Act 2007* (Vic) was recently passed by Victorian Parliament and became operational on 25 July 2007.

The Act amends the *Crimes Act 1958* (Vic), introducing a range of largely technical amendments to the DNA provisions of the *Crimes Act* to enable Victoria to participate effectively in automatic national DNA data matching through the National Criminal Investigation DNA Database. ●

International

NZ: Draft privacy breach guidelines released

27 August 2007. The New Zealand Privacy Commissioner has release new guidelines to help businesses and government organisations take the right steps following a breach of privacy, including notifying people if their personal information has been stolen, lost or mistakenly disclosed.

‘Privacy breach guidelines will help businesses and government organisations manage a privacy breach or suspected breach, and take measures to prevent such breaches occurring in the first place,’ said NZ Privacy Commissioner Marie Shroff.

‘The draft New Zealand guidelines promote the use of best practice consistent with international experience — before we are faced with big breaches of the US kind,’ said Shroff.

New Zealand law does not require privacy breach notification, and the guidelines themselves will not be mandatory. However, Principle 5 of the *NZ Privacy Act 1993* (governing the way personal information is stored) does require all organisations and individuals that hold personal information to take reasonable steps to protect it. This can include notifying people of significant breaches, where necessary. However, Ms Shroff said mandatory breach notification might be considered in NZ in the future.

Further analysis of the draft guidelines will appear in the next issue of the *Privacy Law Bulletin*. ●

Source: NZ Privacy Commissioner media release (27 August 2007).

Google calls for global privacy standards

14 September 2007. Google's Global Privacy Counsel, Peter Fleischer, has called for a discussion about international privacy standards which work to protect everyone's privacy on the internet.

Fleischer that the global nature of business, the growing recognition of privacy rights and increasing technological developments contribute to making the status quo of localised policies no longer acceptable.

'Countries cannot and will not be able to write effective privacy legislation without global cooperation. And as long as there are no global standards for privacy protection, individuals and businesses will remain at risk as they operate online,' said Fleischer.

Fleischer hailed the APEC Framework as the most promising foundation upon which to build global principles.

'The APEC framework already carefully balances information privacy with business needs and commercial interests, and, unlike [the Organisation

for Economic Cooperation and Development guidelines of the 1980s] and the European Directive, it was development in an internet age. Moreover, APEC involves countries with divergent privacy traditions: from Peru to the Philippines, from NZ to Vietnam. Surely, if privacy principles can be agreed upon within the 21 APEC member economies, a similar set of principles could be applied on a global scale.' ●

Source: 'Call for global privacy standards', Google Public Policy blog at <<http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>>.

EU: French court decides on whether an IP address is personal data

12 September 2007. Two decisions of the Paris Appeal Court earlier this year have considered whether an internet protocol (IP) addresses should be considered personal information for the purposes of data protection laws.

The cases originally concerned music counterfeiting using peer-to-peer (P2P) networks. The Paris Appeal Court had to decide on the validity of the first instance procedures regarding the collection of IP address on the P2P network — the individuals against who

the counterfeiting allegations were made claimed that this collection should have been subject to prior authorisation from by the Commission Nationale de l'Informatique et des Libertés (CNIL, France's data protection authority) and, as such authorisation was not obtained, suggested the procedure be nullified.

The Paris Appeal Court rejected these claims, finding that collection of the IP addresses was conducted in full compliance with the law. The court argued that 'the IP address does not allow the identification of the persons who used [the] computer since only the legitimate authority for investigation may obtain the user's identity from the ISP'. As the IP address relates to a machine and not a person, the court concluded, the collection of IP addresses does not constitute a processing of personal data and, thus, prior authorisation from CNIL was not required.

The CNIL was critical of the decision. Among other things, the CNIL noted that the EU Article 29 Working Party of Data Protection Authorities gave its opinion on 20 June 2007 that the IP addresses attributed to an internet user during his or her communications constitutes personal data. ●

Source: *European Digital Rights website*.

PUBLISHING EDITOR: Darren Smith MANAGING EDITOR: Susan Robinson PRODUCTION: Christian Harimanow
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
CUSTOMER RELATIONS: 1800 772 772 GENERAL ENQUIRIES: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood
www.lexisnexis.com.au darren.smith@lexisnexis.com.au

ISSN 1449-8227 Print Post Approved PP 243459/00067

This newsletter may be cited as (2007) 4(4) *Priv LB*

This newsletter is intended to keep readers abreast of current developments in the field of privacy law. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers. This publication is copyright. Except as permitted under the *Copyright Act 1968* (Cth), no part of this publication may be reproduced by any process, electronic or otherwise, without the specific written permission of the copyright owner. Neither may information be stored electronically in any form whatsoever without such permission.

Printed in Australia © 2007 Reed International Books Australia Pty Limited trading as LexisNexis ABN: 70 001 002 357