Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 234093/00011

Reviewing Privacy Law in New South Wales

Michael Tilbury discusses the NSWLRC recommendations on invasions of privacy in anticipation of its report later this year.

Current Privacy Reviews

When the Australian Law Reform Commission (**ALRC**) delivered its report on privacy to the federal Attorney-General at the end of May 2008, two other reviews of privacy in Australasia remained on foot: those of the New South Wales Law Reform Commission (**NSWLRC**) and of the New Zealand Law Commission (**NZLC**). The NSWLRC is planning to report by the end of 2008: the NZLC in late 2009. Meanwhile all three Commissions have published background or consultation papers in response to their respective references.[1]

This article deals with the NSWLRC's reference, focusing on its Consultation Paper, *Invasion of Privacy*, published in May 2007. In that paper the Commission identified a preferred model for a general cause of action protecting privacy on the assumption (that remained to be tested) that it was desirable to introduce greater privacy protection into the law of New South Wales. In its Discussion Paper, *Review of Australian Privacy Law*, published in September 2007, the ALRC picked up the substance of the NSWLRC's preferred model and proposed that there should be a statutory cause of action for invasion of privacy in federal legislation.[2]

The NSWLRC's terms of reference, which in this respect are substantially similar to those of the ALRC, require it to consider the extent to which legislation in New South Wales provides an effective framework for the protection of the privacy of an individual.[3] Unlike the ALRC, however, the NSWLRC is specifically required to consider the 'desirability of introducing a statutory tort of privacy in New South Wales'. In consultation with the ALRC, with which it is charged to liaise, it seemed sensible for the NSWLRC to devote its resources to 'the statutory tort issue' first, since any review of the effectiveness of legislation regulating privacy in New South Wales would necessarily have to take into account the findings of the ALRC in respect of the effectiveness of legislation in protecting privacy across Australia. This is especially so since the terms of reference of the NSWLRC require the Commission to consider the 'desirability of privacy protection principles being uniform across Australia'.

A General Cause of Action for Invasion of Privacy

'General cause of action for invasion of privacy' refers to an action in which an individual claimant seeks redress, generally in the form of compensation, against another individual or some legal person for what is alleged to be a breach of the claimant's privacy. As such, a general cause of action focuses on the role of privacy in private law. In *Invasion of Privacy*, the NSWLRC made two recommendations about such a cause of action: it should be provided for by statute, which would identify the objects and purposes of the statute and contain a non-exhaustive list of the types of privacy invasion that fell within it; and a finding that the claimant's privacy had been invaded would empower the courts in their discretion to award the most appropriate remedy from a legislative catalogue, which would include compensation.[4]

The first recommendation

The first of these recommendations reflects the well-known difficulties of setting the boundaries of privacy with any precision. At base, the difficulties arise because privacy, or its invasion, can comprehend diverse and disparate issues, ranging, for example, from the encroachment on the solitude of an individual (fairly easily describable as an invasion of privacy), to the interference by statute with an individual's ability to access condoms (not so obviously identifiable as an invasion of that individual's privacy).[5] This suggests that the concept lacks coherence. Indeed, even if there is something coherent about privacy, it is difficult to pin down exactly what that is and how it is distinctive of related concepts.

Volume 26 N° 4
July 2008

Inside This Issue:

Focus On Privacy

Communications Law Bulletin

Editors: Matt Vitins, Page Henty & Lesley Hitchens

Printing & Distribution: BEE Printmail

Website: www.camla.org.au

Contents

The best illustration of the difficulty comes from America, where privacy protection in private law originated in a theorised general 'right to privacy' (articulated further as 'the right to be let alone').[6] But this 'right' soon disassembled itself into four specific torts,[7] arguably protecting four separate interests of the plaintiff.[8] Those torts are: unreasonable intrusion on the seclusion of another (whose gist is, arguably, protecting the plaintiff against the intentional infliction of mental distress);[9] the appropriation of the name or likeness of another (arguably protecting the plaintiff's proprietary interest in his or her identity);[10] unreasonable publicity given to another's private life (arguably protecting the plaintiff's reputation);[11] and publicity that unreasonably places another in a false light before the public (also, arguably, protecting reputation).[12]

The practical lesson for law reform is that any statutory definition of privacy that is not circular is bound to be under - or, more likely, over - inclusive. The generality of the circumstances in which an individual ought to have an action for invasion of privacy cannot be identified with greater specificity than those in which the individual has a reasonable expectation of privacy. There seems little doubt that the two American torts of intrusion on seclusion (local or spatial privacy) and publicity given to another's private life (information privacy) identify such circumstances. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, Justices Gummow and Hayne (with whom Justice Gaudron agreed), described these two torts as 'perhaps coming closest to reflecting a concern for privacy "as a legal principle drawn from the fundamental value of personal autonomy"'.[13] And this is reflected in the two recent first instance Australian cases that do protect privacy explicitly at common law and in tort: *Jane Doe v ABC*,[14] which involves a tort of public disclosure of private information; and *Grosse v Purvis*,[15] which involves a tort of intrusion on seclusion, amounting in the case at hand to what is commonly called 'harassment'. This does not, of course, mean that privacy is necessarily only concerned with the terrain of these two torts. It can range wider.

Is a general requirement of a reasonable expectation of privacy in the circumstances sufficient to set boundaries to that range (leaving aside for the moment any other factors that ought to be relevant to establishing a cause of action)? Arguably, it is no more difficult for a court to determine whether, in the circumstances, the plaintiff has a reasonable expectation of privacy than, for example, whether the defendant owed the plaintiff a duty of care in circumstances in which the defendant's conduct has caused purely economic loss to the plaintiff; or whether the conduct of the defendant is false and misleading for the purposes of section 52 of the *Trade Practices Act 1974* (Cth). It is true that, unlike negligence or section 52 cases, there will, initially, be no body of precedent to guide the courts. However, case law will develop, just as it is developing in England,[16] where privacy is now protected (through the action for breach of confidence) within the framework of the *Human Rights Act 1998* (UK), and where it seems reasonably clear that circumstances in which privacy will be protected are those in which the claimant has a reasonable expectation of privacy.[17]

A more substantial criticism of the 'reasonable expectation of privacy' formula is that it provides too ready a protection of privacy. In New Zealand, where there is now a common law privacy tort of unauthorised publication of private and personal information, the action is available if: (1) facts exist in respect of which there is a reasonable expectation of privacy; and (2) publicity is given to those facts that would be considered highly offensive to an objective reasonable person.[18] The second part of the test is drawn immediately from the judgment of Chief Justice Gleeson in *Lenah Game Meats*.[19] That it acts as a real qualification of a test based simply on a reasonable expectation of privacy is illustrated in *Andrews v TVNZ*,[20] a subsequent New Zealand case concerned with the screening on television of footage shot at the aftermath of a motor accident that had occurred on a public road. The victims of the accident were a husband and wife and the footage included expressions of support and love that passed between the couple as they were being rescued. The couple sued for invasion of privacy. Justice Allan held that, although a person has a reasonable expectation of privacy in respect of the sort of conversations that passed between the husband and wife in this case, their publication could not be regarded as highly offensive to an objective reasonable person. The ALRC is of the view that the second part of the test is too restrictive and has suggested that 'substantial offence' should replace 'highly offensive' in the formula.[21]

Whether too restrictive or not, the effect of denying the availability of an action for invasion of privacy in the circumstances of the *Andrews* case is, prima facie, to allow the defendant to publish facts in respect of which the plaintiff has a reasonable expectation of privacy. But only prima facie, because, in New Zealand, a *defence* of legitimate public concern is available to the defendant.[22] Indeed, in *Andrews* itself, Justice Allan held that, even if the publicity given to the facts were considered highly offensive to an objective reasonable person, the action for invasion of privacy would still fail because the defendant could rely on the defence, the rescue and treatment of accident victims being a legitimate concern to the public, since any member of the public may some day stand in need of the service. In this context, then, the application of the defence has the effect of buttressing a particularly important public concern, namely freedom of speech or of expression.

The New Zealand cases illustrate the application to privacy of the methodology of tort law, involving the identification of the ingredients of a cause of action and the specification of defences that can be raised in opposition to it. In the context of privacy, this puts the burden on the defendant of proving that the conduct

or publication that is alleged to invade the plaintiff's privacy promotes the public interest in, for example, freedom of speech. But this raises fundamental questions. Why should public interest be a defence, the burden of which lies on the defendant? Indeed, why should not the burden be on the plaintiff to establish that the success of their action would not infringe the public interest? In short, why should an invasion of privacy be actionable in the first place if, in all the circumstances, the public interest indicates that it should not be? The protection of the public interest in individual privacy frequently provokes conflicts with other public interests. The resolution of such conflicts is not addressed by the separate establishment of the ingredients of a tort and then making out a defence to it. Rather, the factors arguing for and against the application of each interest need to be weighed up against each other to determine which interest is to prevail in the circumstances, a methodology alien to tort law.

A basis must, of course, be found if one interest is to be privileged over another in that balancing process. In the United States, for example, the First Amendment provides justification for preferring interests in free speech over privacy interests. A similar result may flow in New Zealand by reason of the protection of freedom of expression (but not of privacy) in the *New Zealand Bill of Rights Act 1993*. But Australian law provides no basis for balancing these interests other than on a level playing field, as is the case in England where neither the right to private life guaranteed in article 8 of the European Convention on Human Rights and Fundamental Freedoms nor the right to freedom of expression in article 10 have precedence over one another.[23]

As foreshadowed in *Invasion of Privacy*,[24] these considerations have led the NSWLRC to the view that a statutory cause of action for invasion of privacy should provide that a court must take account of the public interest at the outset in determining whether or not there is a reasonable expectation of privacy in the circumstances of the particular case.

The second recommendation

The NSWLRC's second recommendation that a 'remedial smorgasbord'[25] should support the statutory cause of action has two important consequences. First, it gives the court discretion to choose from the prescribed list the remedy that is the most appropriate in all the circumstances, free of the restrictions that may apply to the availability of like remedies at general law. Thus an injunction may be available if, in all the circumstances, it is the appropriate remedy notwithstanding that damages would be an adequate remedy (a condition, however nominal, to the grant of such a remedy at general law). Secondly, it means that rules and principles relating to individual remedies need not necessarily apply to the equivalent remedy listed in the statute. Thus, although the Consultation Paper does envisage the retention of aggravated damages,[26] it is debatable that there will be a need for such damages under the statute if aggravated damages refer to no more than the increased loss that the plaintiff suffers as a result of the defendant's conduct and there is no technical need to identify them as such (for example, to distinguish them from exemplary damages, which the Consultation Paper envisages will not be recoverable).[27]

It remains important to stress that the remedies under the statute will be able to draw analogies as appropriate to like remedies available at general law. For example, as public interest remains an important consideration at the stage of remedy, injunctive relief should be no more capable of being used as a weapon to restrain freedom of speech than it is at general law.[28] Nor, of course, should any other remedy – such as an apology.[29]

Distinguishing the Statutory Regulation of Privacy

The proposed general cause of action for invasion of privacy is to be distinguished from the current statutory regulation of privacy. In New South Wales the broadest regulation of privacy occurs in the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW). The characteristics of the legislation are, first, that its scope is limited to the protection of information (classifiable as 'personal' or 'private'); secondly, that it is not generally aimed at conferring a private right of action on individuals for compensation for its breach, but rather at regulating the collection, storage, access, use and disclosure of the information to which it applies.

Uniformity

The ALRC has made two important proposals about the statutory regulation of privacy in Australia that need to be noted here. The first is its proposal that the *Privacy Act 1988* (Cth) should generally apply to all private sector organisations in Australia.[30] If this proposal is adopted, the most important context in which State privacy legislation would continue to operate is in the handling of personal information by State public sector agencies. Secondly, the ALRC has also proposed the development of Unified Privacy Principles (**UPPs**) that would be applied in State legislation, which would also adopt minimum provisions of federal law.[31]

The enactment of these proposals, as well as the inclusion of a statutory cause of action for invasion of privacy in the federal *Privacy Act*, would result in substantial uniformity of law in Australia. This would be a significant result of the reviews of privacy by the ALRC and the NSWLRC, strengthening the claim of uniformity as an important goal of law reform in Australia – a goal that has been at the forefront of the work of the NSWLRC in the past.[32]

Michael Tilbury is the full-time Commissioner at the New South Wales Law Reform Commission and the Commissioner-in-charge of its privacy reference.

(Endnotes)

1 ALRC: *Review of Privacy*, Issues Paper No 31 (October 2006); *Review of Privacy – Credit Reporting Conditions*, Issues Paper No 32 (December 2006); *Review of Australian Privacy Law*, Discussion Paper No 72 (September 2007); NSWLRC: *Invasion of Privacy*, Consultation Paper No 1 (May 2007); *Privacy Legislation in New South Wales*, Consultation Paper No 3 (forthcoming June 2008); NZLC: *Public Registers*, Issues Paper No 3 (September 2007); *A Conceptual Approach to Privacy*, Miscellaneous Paper No 19 (November 2007); *Privacy: Concepts and Issues (Review of the Law of Privacy Stage 1)*, Study Paper No 19 (February 2008); *Public Registers: Review of the Law of Privacy Stage 2*, Report No 101 (February 2008).

2 Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) vol 1, ch 5 (**ALRC, DP 72**).

3 The terms of reference are set out in NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper No 1 (May 2007), vii (**NSWLRC, CP 1**). Note that the ALRC's terms of reference are not restricted to *individual* privacy.

4 NSWLRC, CP 1, x.

5 See R Wacks, "Why There Never will be an English Common Law Privacy Tort" in A Kenyon and M Richardson, *New Dimensions in Privacy Law* (2006), 154, 175-178.

6 S Warren and L Brandeis, "The Right to Privacy" 4 *Harvard Law Review* 194 (1890), attributing the "right to be let alone" to Judge Cooley: id, 195.

7 *Restatement (Second) of Torts* § 652A.

8 See W L Prosser, "Privacy" 48 *California Law Review* 383 (1960) (**Prosser**), which forms the basis of the law as articulated in the *Restatement*.

9 Prosser, 422.

10 Prosser, 406.

11 Prosser, 398, 422.

12 Prosser, 400, 422-23.

13 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [125], the embedded quotation coming from the judgment of Sedley LJ in *Douglas v Hello! Ltd* [2001] QB 967, [126].

14 [2007] VCC 281.

15 [2003] QDC 151.

16 Especially *Campbell v MGN Ltd* [2004] 2 AC 457. Compare *Wainwright Home Office* [2004] 2 AC 406, *OBG Ltd v Allan* [2008] 1 AC 1, esp [108]-[136], [323]-[329].

17 See especially *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.

18 *Hosking v Runting* [2005] 1 NZLR 1, [117].

19 (2001) 208 CLR 199, [42].

20 [2006] NZHC 1586.

21 ALRC, DP 72, [5.80].

22 *Hosking v Runting* [2005] 1 NZLR 1, [129]-[135].

23 See esp *In re S (a child)* [2005] 1 AC 993, [17] (Lord Steyn).

24 NSWLRC, CP 1, [7.26]-[7.48].

25 The expression is that of Mason P in *Akron Securities v Iliffe* (1997) 41 NSWLR 353, 364.

26 NSWLRC, CP 1, [8.16]-[8.17].

27 NSWLRC, CP 1, [8.11]-[8.15].

28 NSWLRC, CP 1, [8.37]-[8.42].

29 NSWLRC, CP 1, [8.45]-[8.46].

30 ALRC, DP 72, Proposal 4-1. Compare Proposal 4-3.

31 ALRC, DP 72, Proposal 4-4.

32 New South Wales Law Reform Commission, *Guaranteeing Someone Else's Debts*, Report 107 (2006), Rec 4.1 (reforming the law relating to contracts guaranteeing another's debt only makes sense in the context of a uniform law reform initiative).

Eye Spy to Spyware: Working Within the Confines of the NSW Surveillance Devices Act 2007

The New South Wales Surveillance Devices Act 2007 significantly expands the regulation of overt and covert surveillance in New South Wales. Sophie Dawson and Helen Gill take a look.

The New South Wales *Surveillance Devices Act 2007* (the **Act**) received assent from the Governor-General on 23 November 2007 and replaces the *Listening Devices Act 1984* (NSW). It is set to commence on a date to be appointed by proclamation, tentatively set for July 2008, and will apply in conjunction with other New South Wales State and Federal legislation that regulate surveillance devices, including the *Workplace Surveillance Act 2005* (NSW) and the *Telecommunications (Interception) Act 1979* (Cth).

Compared to its predecessor, the Act is broader both in application and effect. In addition to regulating listening devices, its operation extends to optical surveillance, tracking and data surveillance devices.

Listening Devices

Subject to exceptions, the Act prohibits the installation, use or maintenance of a 'listening device' where the device is intended to be used to monitor, record or listen to a private conversation while it is taking place. The prohibition applies regardless of whether the person using the device is a party to the conversation.

'Listening device' is defined broadly under the Act to mean 'any device capable of being used to overhear, record, monitor or listen to a conversation or words being spoken',[1] and is likely to include tape recorders, recording functions on mobile telephones and answering machines, intercoms, baby monitors, parabolic microphones, electronic stethoscopes and telephone wire taps. Hearing aids and similar devices used by persons with impaired hearing to overcome the disability are specifically excluded from the definition.[2] This is consistent with the position under the *Listening Devices Act 1984* (NSW).

Consent and 'lawful interests' exceptions

Two of the exceptions provided under the Act may be of assistance to media organisations. They arise where a party to a private conversation (a person by or to whom words are spoken during the course of the conversation or a person who records or listens to those words with the consent, express or implied, of such a person), uses a listening device to record, monitor or listen to a private conversation and:

- the express or implied consent of all principal parties to the conversation, being persons by or to whom words are spoken during the course of that conversation, is obtained in relation to use of the listening device(s); or
- the consent of one principal party is obtained to use of the listening device(s); and
  - as a matter of objective judgment,[3] the recording of the conversation is reasonably necessary in order to protect the 'lawful interests' of that principal party, being actual 'lawful interests' that are in existence at the time of use of the listening device;[4] or
  - the recording is not made for the purpose of communicating or publishing the conversation (or a report of it) to persons who were not parties to the conversation.

The 'lawful interests' exception is an important one. Over the years a plethora of case law has developed to assist in determining what is encompassed by this phrase, which is not defined in the Act, and was not defined in the *Listening Devices Act 1984* (NSW). The decisions in *R v Zubrecky*,[5] *Violi v Berrivale*[6] and *R v Le*[7] have established that 'lawful interests', synonymous with 'legitimate interests' or 'interests conforming to law' are much broader in scope than mere 'legal interests' in the sense of legal rights, titles, duties or liabilities. The recording of a conversation by a principal party so as to protect him or her from malicious allegations of fabrication as regards the true content of the conversation[8] or the exact terms of an oral contract, where the said terms were outlined during the conversation,[9] have, for example, been found to fall within the scope of 'lawful interests' in particular circumstances. Similarly, the audio-visual recording of one parent's access visits to his or her child for the purpose of protection against allegations of misconduct or impropriety was considered to be a protected 'lawful interest' in a particular case.[10]

However, as noted by Adams J in *R v Le*, this does not mean that:

> the mere intention of making an irrefutable record of a conversation to which one is a party will, without more, satisfy the defence: the circumstances in which the recording occurs will always be relevant to the determination of whether there is, indeed, a 'reasonable necessity' for doing so.[11]

For example, the covert recording of a 'without prejudice' private conversation by a party to that conversation 'for her own private use to assist her comprehension and to give herself an opportunity to revisit what had taken place',[12] while in her lawful interests, has not been found to be reasonably necessary where the interests of that party could have been protected in other ways and without concealment, such as through the taking of handwritten notes.[13]

The 'lawful interests' exception has proved useful in a media context as regards the act of recording; however it does not, of itself, permit publication. In *Channel Seven Perth Pty Ltd v 'S' (A Company)*,[14] for example, Le Miere J found it to be reasonably necessary in the circumstances for 'M', a casual employee of 'S', to protect her 'lawful interests' by using a hidden listening device, at the behest of Channel Seven Perth Pty Ltd, to covertly record a 'private conversation' between herself and the general manager of 'S', in which it was explained that she was to be 'let go' because her pregnancy posed an 'occupational health and safety risk'. Le Miere J explained that while the video did not 'record' unlawful conduct, it 'is or may be evidence from which it may be inferred that the company acted unlawfully'[15] by discriminating against 'M' on the grounds of her pregnancy. However, while Le Miere J found the recording to be lawful, he ultimately refused Channel Seven Perth Pty Ltd's application[16] for an order allowing *publication* of the record of private conversation as, having weighed the competing

interests, he was not satisfied that the publication would further or protect the public interest (the test in Western Australia).

On appeal to the Supreme Court of Western Australia, McLure JA (with whom Pullin and Buss JJA agreed) held that Le Miere J had erred in going outside the scope and purpose of the Act in weighing up the competing interests and considering the public interest in protecting the privacy of the general manager's conversation, and the likely damage to the general manager and 'S' by publication of the interview.

The Supreme Court of Western Australia set aside Le Miere J's decision and determined the matter afresh, finding that as the recording did not record unlawful conduct and Channel Seven Perth Pty Ltd could broadcast the story without the covertly recorded interview, 'the evidence falls well short of providing a proper foundation for a conclusion that the proposed publication should be made to protect or further the public interest.'[17] The appeal was dismissed, as was Channel Seven Perth Pty Ltd's further appeal to the High Court of Australia.[18]

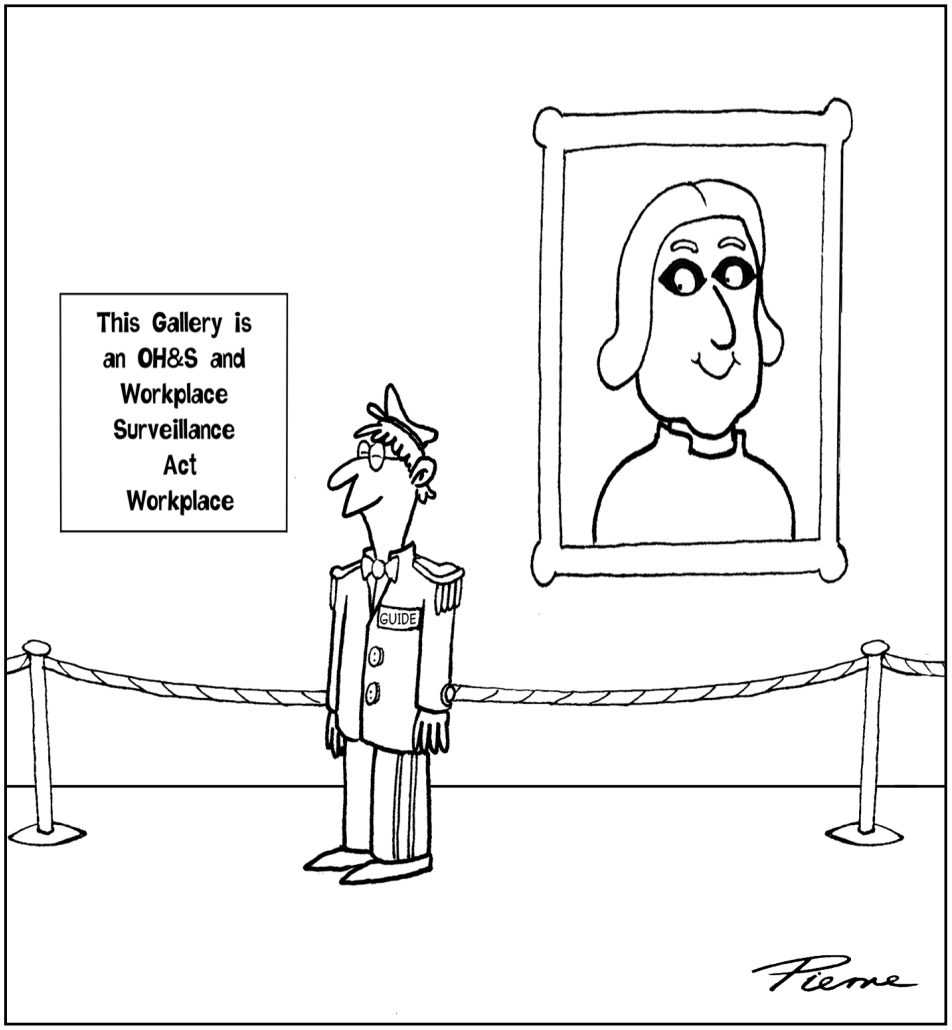
While there is no equivalent to section 31 in the NSW Act, publication by the media of a record of private conversation made by a listening device will generally only be permitted with the express or implied consent of all principal parties to the private conversation.

The practical effect of the Act for journalists, private investigators, parents and other individuals who wish to use a listening device to listen to, record or monitor a private conversation to which they are not a party, is substantially the same as under the *Listening Devices Act*. That is, unless the consent of one or more principal parties to the conversation is obtained or the 'lawful interests' exception applies, then use of a listening device to record a private conversation will constitute an indictable offence. Under the Act, the maximum penalty is two years imprisonment and/or an $11,000 fine for an individual, and a $22,000 fine in respect of a body corporate.

Further, recordings or reports of 'private conversations' recorded in contravention of the Act may be inadmissible in evidence in civil or criminal proceedings by virtue of section 138 of the *Evidence Act 1995* (NSW). This is an important consideration for journalists, since this could make recordings of no use as a defence in defamation proceedings.

Optical Surveillance Devices

The Act also prohibits the installation, use or maintenance of optical surveillance devices on or within premises, a vehicle, or any other object for the purpose of observing or recording the carrying on of an activity, where the installation, use or maintenance involves entry onto premises or entry into or interference[19] with a vehicle or object without the express or implied consent of the owner or occupier of the premises or the individual having lawful possession or control of the vehicle or object.



'Optical surveillance device' is defined broadly in the Act to mean 'any device capable of being used to record visually or observe an activity',[20] and is likely to include binoculars, telescopes, cameras, video cameras, security cameras, closed-circuit television (CCTV) and webcams. However, glasses, monocles, contact lenses and similar devices used by persons with impaired sight to overcome the disability are specifically excluded from the definition.[21]

Through limiting the application of the prohibition to activities that involve a non-consensual entry onto premises or into vehicles or interference with objects, the Act effectively constrains but does not prevent the use of optical surveillance devices for the purpose of investigative journalism. Nor does it stop private investigators from surveying and recording the movements of their quarry, provided that they work within the limitations of the Act.

Cases concerning the law of trespass will be very important in understanding when use of a camera is likely to be lawful under the Act. In *TCN Channel Nine Pty Ltd v Anning*,[22] for example, a television news crew entered a residential property with the intention of filming a police raid on the premises and conducting interviews with a view to broadcasting. At first instance, District Court Judge English found that TCN Channel Nine Pty Ltd, by its servants and agents, did not have any express or implied licence to enter and remain on the property to film. Thus, in so doing, it had committed the tort of trespass to land and caused the occupier (Anning) personal injury including mental trauma. The occupier was awarded damages in the amount of $100,000 (being general, aggravated and exemplary damages) plus interest. On appeal, the New South Wales Court of Appeal (Spigelman CJ, Mason P and Grove J) unanimously upheld the decision of English DCJ as regards the finding of trespass to land, but allowed the appeal insofar as exemplary damages and damages for mental trauma were awarded, and the interest calculated. Ultimately Anning was awarded damages in the amount of $50,000 (being general and aggravated damages) plus interest.

While the courts do recognise an implied licence to enter a property to approach the

occupier to request permission to film,[23] an implied licence was not found to exist in *TCN Channel Nine Pty Ltd v Anning*. This was because the Court found that TCN Channel Nine Pty Ltd, by its servants and agents, had entered the property with the intention of filming the police raid as distinct from requesting permission to film.

The use of non-malicious Trojan horse programs creates an interesting scenario. These are programs that are typically installed to manage systems, detect suspicious data, deploy and patch software, and conduct surveillance and forensics. They may be installed directly, remotely via an email attachment, or through exploiting common operating system vulnerabilities and bypassing security measures.

The question arises as to whether the covert use of a non-malicious Trojan horse program, installed remotely via an email attachment or by exploitation of common operating system vulnerabilities, that intercepts or even initiates a webcam feed, will constitute a breach of the Act.

While it is arguable that such an activity would constitute interference with a computer (an object) and that it would contravene the Act on that basis, the position is not free from doubt. There are, of course, also other laws which would need to be taken into account in relation to any such activity, including any right of action for breach of privacy,[24] Federal, State and Territory computer crimes legislation (where relevant) and, depending on the person using the software in question, workplace surveillance and/or privacy legislation.

Such activities, if carried out with an intention to commit an indictable offence, would be likely to contravene section 308C of the *Crimes Act 1900* (NSW).

Tracking Devices

The Act prohibits installation, use or maintenance of a 'tracking device' for the purpose of ascertaining the geographical location of a person or object without the express or implied consent of that person or the person having lawful possession or control of the object, unless it is for a lawful purpose.

The breadth of the definition of 'tracking device' provided in the Act, and the fact that it includes 'any electronic device *capable* of being used'[25] for such a purpose, means that it is likely to include such devices as global positioning system chips found in vehicles and mobile telephones, as well as terrestrial-based automatic vehicle location systems (such as LoJack and LORAN) and other devices capable of determining the geographical location of a person or object.

The phrase 'lawful purpose' is not defined in the Act. However in *Taikato v R*[26], it was determined that 'lawful purpose' is not synonymous with 'lawful authority', but is a purpose that is authorised in a positive rule of law 'as opposed to not forbidden by law.'[27] Similarly, *The Macquarie Dictionary*, the dictionary of reference for Australian courts, defines 'lawful' to mean 'allowed or permitted by law', 'legally … entitled' and 'recognised or sanctioned by law'.[28]

In determining the practical effect of this prohibition, consideration must be given to section 275A of the *Telecommunications Act 1997* (Cth). Section 275A deems information about the location of a mobile telephone handset or other mobile communications device to be information relating to the affairs of the customer responsible for the handset or device. Section 276 of that Act prohibits use and disclosure of such information by carriers, carriage service providers and telecommunications contractors, subject to exceptions. The key exception, in section 289, is where the person to whom the information relates consents to the use or disclosure, or is reasonably likely to be aware that information is used or disclosed in the circumstances in question.

Data Surveillance

The final prohibition in the Act concerns the installation, use or maintenance of a data surveillance device(s) for the purpose of recording or monitoring the input and/or output of information from a computer where such an act entails the entry onto premises or interference[29] with a computer or network in the absence of the express or implied consent of the owner or occupier of the premises or the individual having lawful possession or control of the computer or computer network.

'Data surveillance device' is defined broadly in the Act to mean 'any device or program capable of being used to record or monitor the input of information into or output of information from a computer'[30] other than an optical surveillance device. 'Computer' is also defined broadly to mean 'any electronic device for storing, processing or transferring information',[31] and is likely to include Blackberrys, Blackjacks, Palm Pilots and similar hand-held devices.

As the prohibition is limited to acts that entail entry onto premises or interference with a computer or computer network without consent, employers retain the capacity under the Act to utilise non-malicious Trojan horse programs, such as Microsoft's soon to be patented Anti-slacking software, to overtly monitor internet usage, employee productivity, competence and physical well-being,[32] and to log keystrokes. Such surveillance is also regulated by the *Workplace Surveillance Act 2005* (NSW), and employers must comply with notice requirements regarding such surveillance.

The question arises as to whether non-malicious Trojan horse programs that are used to covertly spy on a computer user, log keystrokes to steal information such as passwords and credit card numbers, and report data by sending it to a fixed email or IP address, would involve 'interference' with a computer or network given that it would not interfere with or delay normal computer operations. A recent example of such a program, according to media reports, is the specially crafted Excel file that, if downloaded from an email attachment by an individual with a pre-2007 version of Microsoft Excel, permits the sender to obtain access to the target computer for malicious purposes.[33]

The question of what constitutes 'interference with a computer or computer network' was considered in *The Queen v Steven George Hourmouzis*[34] in which the defendant pleaded guilty to interfering with, interrupting or obstructing the lawful use of a computer contrary to section 76E of the *Crimes Act 1914* (Cth). Mr Hourmouzis had sent more than three million spam email messages to addresses in Australia and overseas fraudulently extolling a predicted 'plus 900 per cent rise in Rentech stock over the next few months', that were relayed through third party servers to minimise the risk of detection. The utilisation of these servers, while not causing any physical damage, did require the servers to be shut down and time to be lost so that the offending messages could be cleared. Further, the trading of Rentech shares on the NASDAQ had to be halted pending an announcement by the company, financial and personal resources had to be expended to investigate the spam problem, anti-spam defences had to be implemented and complaints dealt with, and certain internet addresses had to be blocked for a period, all of which affected the ability of those businesses to communicate.

Such repercussions would likely constitute interference with a computer or computer network under the Act. They may also contravene section 308C of the *Crimes Act 1900* (NSW) (referred to above) if there is the requisite intention to commit, or facilitate the commission of, a serious indictable offence within the jurisdiction of New South Wales.

Prohibition on Disclosure and Possession of Records and Recordings

The Act prohibits natural persons and bodies corporate from publishing or communicating to any person, any record, recording or information that has come to their knowledge as a direct or indirect result of the use of a surveillance device in contra-

vention of Part 2 of the Act,[35] *unless* the publication or communication is made:

- to a party to the private conversation or activity;
- with the express or implied consent of all principal parties to the conversation or activity;
- to the person in lawful possession or control of the computer or computer network, or with their express or implied consent; or
- some other exception applies.

Further, the mere possession of a record of a private conversation or activity will constitute an offence under the Act where the individual or body corporate with possession has knowledge (as distinct from a mere suspicion) that the record was obtained through the direct or indirect use of a listening device, optical surveillance device or tracking device in contravention of the Act,[36] *unless* such possession is:

- in connection with proceedings for an offence against the Act or its regulations (if and when they are enacted);
- with the consent of all parties involved in the conversation or activity; or
- the result of communication or publication of the record in circumstances that do not constitute a breach of the Act.

The latter prohibition is of particular significance for journalists as an offence will be committed regardless of whether the journalist actually uses or discloses the record. This prohibition is consistent with section 8 of the *Listening Devices Act 1984* (NSW), although its application is extended to activities recorded using optical surveillance devices. Journalists should, therefore, promptly obtain advice if they receive a record which may fall into this category.

It is notable that none of these prohibitions contain any exception for circumstances in which there is a strong public interest in publication, such as where surveillance exposes corruption. This is a significant matter for journalists, as it may, in some cases, prevent or limit the media's ability to expose such matters.

Conclusion

The Act significantly expands the regulation of overt and covert surveillance in New South Wales. Interesting questions arise as to whether it strikes the balance between privacy interests and the public interest in effective investigative journalism, and how it will operate in relation to new technologies. The second of these issues will, no doubt, be resolved by courts over time.

Sophie Dawson is a Partner and Helen Gill a Graduate Lawyer in the Sydney office of Blake Dawson.

(Endnotes)

1 Section 4 of the Act.

2 Section 4 of the Act.

3 *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580 at 585-86 (Branson J).

4 *Amalgamated Television Services Pty Ltd v John Marsden* [2000] NSWCA 167; BC200003896 at [21], citing Levine J.

5 (unreported, NSWDC, Graham J, 22 February 1991) at p 14.

6 (2000) 99 FCR 580 at 587 (Branson J).

7 (2004) 60 NSWLR 108

8 *R v Zubrecky* (unreported, NSWDC, Graham J, 22 February 1991) at p 14.

9 *Violi v Berrivale* (2000) 99 FCR 580 at 587 (Branson J).

10 *Director of Public Prosecutions v Nakhla* [2006] NSWSC 781; BC200605999.

11 (2004) 60 NSWLR 108 at [84] (Adams J).

12 *See v Hardman* [2002] NSWSC 234; BC200201585 at [21] (Bryson J).

13 *R v Le* (2004) 60 NSWLR 108 at [84] (Adams J).

14 (2005) 30 WAR 494; [2005] WASC 175; BC200505885

15 *Channel Seven Perth Pty Ltd v 'S' (a company)*, as above at [36] (Le Miere J).

16 Section 31(1) of the *Surveillance Devices Act 1998* (WA) provides that:

> … a judge may make an order that a person may publish or communicate a private conversation or a report or record of a private conversation, or a record of a private activity that has come to the person's knowledge as a direct or indirect result of the use of a listening device or an optical surveillance device under Division 2 or 3, if the judge is satisfied, upon application being made in accordance with section 32, that the publication or communication should be made to protect or further the public interest.

17 *Channel Seven Perth Pty Ltd v 'S'* at [41] (McLure JA).

18 *Channel Seven Perth Pty Ltd v 'S' (a company)* [2007] HCATrans 628.

19 The word 'interfere' is not defined in section 4 of the Act. *The Macquarie Dictionary* (3rd edn, 1998) defines interfere to mean 'to come into opposition, as one thing with another, especially with the effect of hampering action or procedure'. Similarly, in *Fitzpatrick v Day* (1990) 54 SASR 186, Duggan J held (at 189) that the interference in question does not have to be such as to cause 'damage or some sort of alteration to the character or nature of the item in question', there need only be 'the interruption of a regular or intended course of events: a "coming between"'.

20 Section 4 of the Act.

21 Ibid.

22 (2002) 54 NSWLR 333.

23 *Robson v Hallett* [1967] 2 QB 939.

24 See, for example, *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, *Jane Doe v Australian Broadcasting Commission* [2007] VCC 281, *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706, *Kalaba v Commonwealth* [2004] FCAFC 326; BC200408581 and *Kalaba v Commonwealth* [2005] HCATrans 478.

25 Section 4 of the Act.

26 (1996) 186 CLR 454

27 *Taikato v R* [1996] 186 CLR 454 at 460 and 463 (Brennan CJ, Toohey, McHugh and Gummow JJ).

28 *The Macquarie Dictionary* (3rd edn, 1998).

29 See above n 16.

30 Section 4 of the Act.

31 Ibid.

32 'Anti-slacking software at work' *Sydney Morning Herald*, 17 January 2008; 'Microsoft files "Big Brother" patent in the US' *Intellectual Property Newsletter*, February 2008.

33 'Hackers exploit security hole in Excel' *Sydney Morning Herald*, 17 January 2008.

34 (Victorian County Court, 30 October 2000 (Unreported))

35 Sections 11 and 14 of the Act.

36 Section 12 of the *Listening Devices Act*.

Privacy 2.0: Online Privacy in a User-generated World Wide Web

Andrew Ailwood and Chris Govey look at the difference between younger and older Web users when it comes to privacy.

Web 2.0 was spawned from a change in attitude amongst software developers rather than any single technical revolution.[1] The resulting proliferation of user generated content on social media sites such as Wikipedia, YouTube and personal blogs, and increased user interaction through social networking sites such as Facebook, MySpace and Bebo, has led to a rethink of many key regulatory axioms.

In particular, Web 2.0 has fostered a change in users' attitudes towards their privacy.[2] According to Chris Kelly, Facebook's chief privacy officer, the classic notion of the right to privacy as the user's right 'to be left alone' has been replaced by a focus on users' ability to control their personal information.[3] In essence, users are resigned to the inevitability of, and indeed facilitate, the release of their personal information into the public domain; however, they expect that release to be accompanied by a right to privacy that controls how that personal information may be used.

On 30 May 2008, the Australian Law Reform Commission (the ***ALRC***) was due to deliver its eagerly awaited final report and recommendations to the Federal Attorney-General (the ***ALRC Report***) following the ALRC's *Review of Australian Privacy Law*.[4] While the content of the ALRC Report is not yet publicly available,[5] it is expected to address the growing gap between the technicalities of the law of privacy in Australia and the technologies utilised by the private citizens of Australia.[6]

In this expectant period leading up to the release of the ALRC Report, this article discusses the shift in (particularly young) users' attitudes towards privacy that has given Australia the phenomenon of 'Privacy 2.0'. We give particular attention to the use of personal information by advertisers and the possible enforcement options that might be included in amendments to the *Privacy Act 1988* (Cth) (the ***Privacy Act***). Ultimately, regulators must join users in recognising that, as there is no way to guarantee absolute privacy online, the focus of privacy laws must be ***controlling*** the use of personal information, rather than ***preventing*** its use and disclosure outright.

Targeting Advertising

The increasing prevalence and penetration of Web 2.0 is perhaps best reflected in the amounts recently paid by:

- News Corporation to purchase MySpace (US$580 million in July 2005);[7]
- Google Inc to become the exclusive advertisement provider for News Corporation owned sites (including MySpace) for three years (US$900 million in August 2006);[8]
- Microsoft Corporation to purchase a 1.6% stake in Facebook (US$240 million in October 2007);[9] and
- AOL to purchase Bebo (US$850 million in March 2008).[10]

These figures reveal the commercial value of sites that are constantly collecting personal information. Web 2.0's advertising potential resides in the approximately 115 million 'unique' viewers that, for example, MySpace and Facebook each attract to their respective sites every month.[11] Indeed, a study published in March 2007 by Pali Research analyst Richard Greenfield estimated that MySpace generates over US$70 million a month in advertising revenue.[12]

This advertising potential is being extended by developing marketing techniques. Modern sites hyper-target advertisements to users based on their self professed demographic information and the content of a page that they are viewing. For example, where the user is male and using a Sydney IP address to search for information on cricket, it is reasonable to assume that they might be interested in purchasing tickets to a match at the Sydney Cricket Ground. Therefore, an advertisement server using hyper-targeting would advertise an upcoming game at the Sydney Cricket Ground.

More interesting is when advertisers use Web 2.0 to extrapolate users' interests, demographics and use history to classify them into market segments and serve up advertisements accordingly. For example, where the user is male and using a Sydney IP address to look for information on cricket, it is reasonable to assume that they might be susceptible to an advertisement for beer based on the generalised market segment that their details classify them in.

Each of these advertising techniques relies on unidentified information which, as disclosed to advertisers in an aggregate form, is arguably outside the scope of the Privacy Act definition of 'personal information'. However, the next advance in targeted marketing involves selecting those users whose network of friends (as indicated by the structure of their Facebook or MySpace account) reveals them to be a leader or influential personality type, with a correspondingly strong influence on the (purchasing) behaviour of their social circle (or, more likely, circles). Such information is inherently sensitive but arguably (without being attached to traditional identifying detail) falls outside the ambit of the protection of the National Privacy Principles (***NPPs***) in the Privacy Act[13] as it is not 'information or an opinion… about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion'.[14] The question of policy then becomes whether such use of behavioural and psychological data should be subject to a regulatory regime which facilitates rights of access and security and limits the use and disclosure of such data.

Rather than rebelling against this increasing use of users' personal information, Web 2.0 users in a Privacy 2.0 Australia are more likely to prefer to receive advertisements that are targeted to their interests. The ALRC notes that: '[y]oung people appear much more willing to share personal details, post images and interact with others on internet chat sites'.[15] Users are happy to trade their personal information for a perceived benefit; whether it be pure pleasure, a chance at winning the latest computer hardware to facilitate their future browsing or merely so that the unavoidable online advertisements they view are at least tailored to their interests. Indeed, the growing prevalence of such targeted advertisements must be supported by a growth in 'hits' on such advertisements, which is in turn indicative of users' preference for targeted advertising material.

Take-down Notices or Statutory Cause of Action for Privacy Breaches

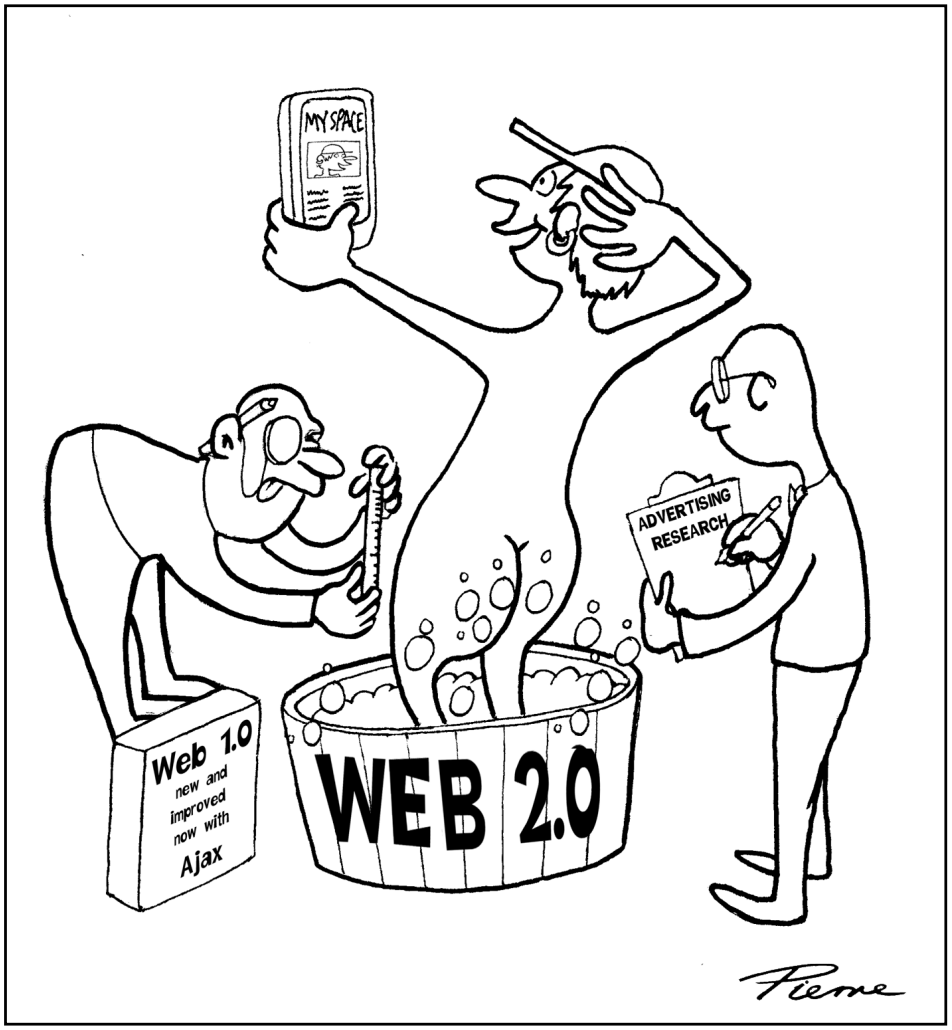
Despite the positive aspects of increased access to Web 2.0 users' personal information discussed above, there are clearly instances where users desire greater con-

trol. One popular feature of social networking sites such as Facebook and MySpace is that they permit users to post photos. As Duncan Watts (a sociologist at Columbia) opined in an interview with The New Yorker in 2006: '[i]f I had to guess why sites like Facebook are so popular, I would say it doesn't have anything to do with networking at all. It's voyeurism and exhibitionism. People like to express themselves, and they are curious about other people.'[16]

The risk is that there will come a time when the user feels it is necessary to restrict the use of their personal information. Just as David Hicks probably regrets posing with a bazooka on his shoulder, and Trevor Flugge no doubt would have preferred that the photo of him shirtless with a revolver in his hand had remained private, how many Web 2.0 users wake up on Saturday morning fearful of the personal information their friends might be about to post online? Perhaps it is fair to say, as the founder and current CEO of Facebook Mark Zuckerberg did in 2006 (regarding students who had been expelled from school as a result of photos of them taking illicit drugs being posted on Facebook): 'I think that that's just the sort of deviant behaviour on the very far end of the distribution'.[17] But at what point does a photo that is damaging to one's reputation, and uncontrollable once released, foster a legitimate privacy concern?[18]

In the internet's infancy, users operated under a screen name or pseudonym, but as the internet pervades the offline, real lives of users, those users have shown an increasing willingness to utilise their real name (in exchange for otherwise unattainable benefits, such as online shopping deliveries or online job applications).

However, with this departure from anonymity comes the risk of real damage to users' reputations and their ability to control their public information. Currently, the law does not provide for an effective, let alone timely, solution. Beyond a desperate appeal to the 'friend' that posted the offending photo, the user has no obvious legal recourse. Although an image is personal information so long as an individual's identity is apparent or can be reasonably ascertained from that image,[19] it will not be regulated by the Privacy Act if it was taken by an individual who is acting in their private capacity,[20] or by someone acting on behalf of a small business which is exempted from the Privacy Act.[21] Even if the Federal Privacy Commissioner (the ***FPC***) investigated the organisation hosting the personal information, a subsequent court order (from the Federal Court or the Federal Magistrates Court) would be required to enforce any determination by the FPC that there has been a breach of privacy.[22]



It is in this context that the ALRC has discussed introducing a take-down scheme similar to that governed by the Australian Communications and Media Authority regulations in the context of online adult content.[23] This could be extended to material that interferes with a user's privacy. While many Web 2.0 sites have developed terms of use that provide for a voluntary take down scheme following notice by users of the existence of offensive content, or even proactively moderate content, a legislated take-down scheme may provide a 'practical, cost-effective remedy for individuals faced with publication of offensive material, including images, relating to themselves. It would enable individuals to exercise some control over how images of themselves are published when they are taken without consent.'[24]

Additionally, the ALRC has considered a statutory cause of action for invasion of privacy, describing it as 'the most effective way to regulate the issue'.[25] This would also give a user direct recourse against the individual posting the photo. Such recourse would be particularly pertinent to Australian users faced with the prospect of having personal information removed from a site hosted by an organisation that is not incorporated or otherwise formed in Australia. Generally speaking, the Privacy Act only applies to such organisations if they are carrying on business in Australia and, even then, only applies in relation to the organisation's acts and practices in Australia.[26] If the relevant personal information was never collected or held in Australia then it may not be covered by the Privacy Act.

Not only might a take-down notice scheme or a statutory cause of action overcome this jurisdictional obstacle; such measures would also provide a pragmatic solution to privacy enforcement between the extremes of an outright ban on cameras in public on the one hand and the arguably toothless provisions of the current Privacy Act on the other. Moreover, a take-down notice scheme or a statutory cause of action would bring Australian law into line with Privacy 2.0 by providing users themselves with the tools to control their personal information.

Conclusion

As the increasingly commercial use of personal information by advertisers and the potential viability of a take-down notice scheme (or even a statutory cause of action for privacy breaches) suggest, there has been a significant shift in users' attitudes

towards privacy since the inception of the internet. Although the ALRC recognises that 'individual control is a more viable regulatory option than technical legal solutions',[27] and that 'young people think of privacy differently from older generations',[28] it seems likely that the ALRC Report will not capitalise on this change in Web 2.0 users' attitudes towards privacy to update Australian privacy law in line with Privacy 2.0. The ALRC believes that '[w]hile young people have slightly different privacy concerns and experiences when compared to older Australians, the differences are not so great as to warrant a reconsideration of the basic framework of the Privacy Act...'.[29]

Regardless of the recommendations encapsulated in the ALRC Report once released, and irrespective of the precise amendments (if any) passed by the Federal parliament, it is undeniable that the shift in users' attitudes that underscores Privacy 2.0 will only gain momentum as the generations of young people that take technology for granted grow older.

Andrew Ailwood is a Senior Associate and Chris Govey a Law Graduate in the Sydney office of Allens Arthur Robinson.

(Endnotes)

1 Wikipedia, 'Web 2.0', http://en.wikipedia.org/wiki/Web_2 (last accessed 25 June 2008).

2 This article, in line with the Australian Government Law Reform Commission's '*Review of Australian Privacy Law: Discussion Paper*' (September 2007, Discussion Paper 72 (the ***ALRC Discussion Paper***), focuses on information privacy, that is the 'establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records' (known as 'data protection'), as opposed to bodily privacy ('the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches'), privacy of communications (that is the 'security [and prevention of interception] of mail, telephones, email and other forms of communication') and territorial privacy ('the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes trespass, searches, video surveillance and ID checks') – see the 'defining privacy' section of the ALRC Discussion Paper (page 114).

3 ALRC Discussion Paper, pages 1730-31.

4 ALRC Discussion Paper.

5 The ALRC Report will not be publicly available until it is tabled in Parliament; the ALRC believes this will occur in August 2008.

6 To this end, '[i]mportant definitions in the Privacy Act—such as the definition of 'personal information', 'sensitive information' and 'record'—should be updated to deal with new technologies and new methods of collecting and storing personal information' (ALRC Discussion Paper, page 105); in particular, the ALRC recognises that reliance on the *Acts Interpretation Act 1901* (Cth) to extend the definition of 'record' to computer data is inadequate (see page 218 of the ALRC Discussion Paper). Similar recognition should be given to the possibility of a users' IP address constituting personal information as other information accretes around it (see page 205 of the ALRC Discussion Paper).

7 News Corporation, 'News Corporation to Acquire Intermix Media, Inc', (18 July 2005), http://www.newscorp.com/news/news_251.html (last accessed 25 June 2008).

8 News Corporation, 'Fox Interactive Media enters into Landmark Agreement with Google Inc', (7 August 2006), http://www.newscorp.com/news/news_309.html (last accessed 25 June 2008).

9 Jay Greene, 'Microsoft and Facebook Hook Up' (25 October 2007) http://www.businessweek.com/technology/content/oct2007/tc20071024_654439.htm (last accessed 25 June 2008).

10 Allen Stern, 'Bebo To AOL for $850 Million', (13 March 2008), http://www.centernetworks.com/aol-acquires-bebo-850-million (last accessed 25 June 2008).

11 Michael Arrington, 'Facebook No Longer The Second Largest Social Network', (12 June 2008), http://www.techcrunch.com/2008/06/12/facebook-no-longer-the-second-largest-social-network/ (last accessed 25 June 2008).

12 Diane Mermigas, citing Richard Greenfield, 'Make Social Networks Pay: Recast Ads', (18 April 2008), http://blogs.mediapost.com/on_media/?p=151 (last accessed 25 June 2008).

13 The NPPs are contained in Schedule 3 of the Privacy Act. The breach of an NPP by an organisation, such as a web hosting site, is a contravention of section 13A(1)(b)(i) of the Privacy Act).

14 See section 6(1) of the Privacy Act for the definition of 'personal information'.

15 ALRC Discussion Paper page 122, citing L Weeks, 'See Me, Click Me: The Publizen's Life? It's an Open Blog. The Idea He May be Overexposed? LOL', *Washington Post (online)* (23 July 2006) <www.washingtonpost.com>.

16 John Cassidy, 'The Online Life: Me Media: How hanging out on the internet became big business' (15 May 2006) The New Yorker, page 50, 55.

17 Id, page 50, 59.

18 Pertinently, the ALRC Discussion Paper notes (at page 119) that '[r]ecently enacted domestic human rights legislation also recognises privacy as a basic human right. For example, s 13 [privacy and reputation] of the *Charter of Human Rights and Responsibilities Act 2006* (Vic)' and the *Human Rights Act 2004* (ACT).

19 See the definition of 'personal information' in section 6(1) of the Privacy Act.

20 Sections 7B(1) and 16 of the Privacy Act.

21 ALRC Discussion Paper, page 1735.

22 ALRC Discussion Paper, page 180.

23 Currently set out in the *Broadcasting Services Act 1992* (Cth) schedules 5 and 7.

24 ALRC Discussion Paper, page 1747.

25 ALRC Discussion Paper, page 1747.

26 In relation to any act or practice outside Australia the organisation must also comply with the rules on transborder data flow in NPP 9.

27 ALRC Discussion Paper, page 1744.

28 ALRC Discussion Paper, page 1715.

29 ALRC Discussion Paper, page 1744.

Murray v Big Picture UK Ltd: An Image Right for the Children of Celebrities?

Recent decisions in the UK and Europe that deal with the rights of public people to private lives are looking at how it might be different for children. Anne Flahvin reviews the situation.

Introduction

In a decision with potentially enormous consequences for the development of privacy law in the UK, the English Court of Appeal has reinstated a claim for breach of privacy in respect of a photograph taken of author JK Rowling's infant child while out in public with his parents.

While the claim has yet to be heard, the decision of the Court of Appeal in *Murray v Big Picture UK Ltd*[1] to overturn the earlier strike out has raised for consideration the question whether English law recognises a right of privacy in respect of photographs of a child taken in a public place that convey nothing sensitive or 'private' about the child. According to the Court of Appeal, it is at least arguable that children of famous parents have a reasonable expectation not to be photographed in public, however innocuous the photograph.

If the claim is ultimately successful, the English courts will have all but created an image right for the children of celebrities. [2]

The Murrays' breach of privacy claim

Dr David Murray and his wife Joanne Murray (aka Harry Potter author JK Rowling) were walking from their Edinburgh flat to a local café with their infant son David - who was being pushed in his pram - when they were photographed without their knowledge or consent.

Several photos were taken, including a photograph which was later published in the *Sunday Express* newspaper accompanied by the headline: 'My Secret' and the text of a quotation from Mrs Murray in which she set out some of her thoughts on motherhood and family life.

The Murrays commenced proceedings against the newspaper and Big Pictures Ltd (the photographic agency responsible for the photograph) on behalf of David seeking an injunction restraining further publication and damages or an account of profits for breach of confidence, the infringement of his right to privacy and the misuse of private information relating from the taking, recording, holding and publication of the photograph. The newspaper compromised its claim, so that proceedings continued only against Big Pictures Ltd.

Big Pictures Ltd applied to have the claim struck out on the basis that it had no reasonable prospects of success.

First instance strike out decision

Before considering Patten J's first instance decision,[3] it is useful to briefly review two important decisions – one a decision of the House of Lords and the other a decision of the European Court of Human Rights – which were crucial to any consideration of the Murrays' claim.

Following the introduction in 2000 of the *Human Rights Act* 1998, which required English courts to give effect to the rights protected by Articles 8 (privacy) and 10 (freedom of speech) of the European Convention of Human Rights, the courts had developed the cause of action for breach of confidence to include private information which would not previously have been regarded as confidential.

In *Campbell v Mirror Group Newspapers*,[4] the House of Lords held by a three-to-two majority that an action for breach of confidence arose in respect of the publication of photographs taken in a public place. In that case, model Naomi Campbell was awarded damages in respect of a photograph of her leaving a Narcotics Anonymous meeting and an accompanying story containing details of her treatment. For the majority in *Campbell's* case, what made the activity that was photographed 'private', and therefore subject to protection, was that it conveyed information relating to therapeutic treatment. Lord Hope said:

> *If the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected.*[5]

The Court was at pains, however, to stress that it was ***not*** recognising a right to control one's own image, absent some private information being conveyed. Baroness Hale put it this way:

> *The activity photographed must be private. If this had been, and had been presented as, a picture of Naomi Campbell going about her business in a public street, there could have been no complaint. She makes a substantial part of her living out of being photographed looking stunning in designer clothing. Readers will obviously be interested to see how she looks if and when she pops out to the shops for a bottle of milk. There is nothing essentially private about that information nor can it be expected to damage her private life. It may not be a high order of freedom of speech but there is nothing to justify interfering with it.* [6]

Shortly after *Campbell's* case, the European Court of Human Rights took a more expansive approach to the question of whether photographs taken in a public place which convey nothing sensitive or private about an individual are nevertheless capable of being subject to a claim for breach of privacy.

In *Von Hannover v Germany*,[7] Princess Caroline of Monaco appealed against the refusal of German courts to grant her an injunction restraining further publication of photographs of her which had been published in various German magazines. All the photos had been taken in public places. They included photos of the Princess in a restaurant, riding a horse and on a skiing holiday; in other words, going about her daily life. The claim failed before the German courts due to a doctrine of German law that provided that 'figures of contemporary society *par excellence*' could only claim protection for privacy if the intrusion complained of occurred at their home or in a secluded place away from the public gaze.

The European Court held that to the extent that German domestic law deprived Princess Caroline of a remedy in respect of the photographs complained of, the law was in violation of Article 8 of the European Convention of Human Rights. The Court was critical of the German domestic courts for attaching 'decisive weight' to freedom of the press and to the public interest in knowing how Princess Caroline behaved outside of her official functions.[8] While the Court stressed that freedom of expression constitutes one of the essential foundations of a democratic society, it was clearly of the view that 'the entertainment press' was not deserving of the same level of protection as publishers of 'news items of major public concern'.[9]

In characterising the activities which were photographed as 'private', the Court appears to have been drawing a distinction between the 'public' life of a public figure – such as the carrying out of official duties – and the private, day-to-day life of such a person. On the

test set down by the Court in *Von Hannover*, a public figure has a reasonable expectation of privacy with respect to the latter, even if the activities in question are carried out in public. Unless the publication can be justified on the basis that it is capable of contributing to debate in a democratic society, the Article 8 interest will generally prevail over any interest in freedom of speech.

When Big Pictures' strike out claim came before him in June 2007, Patten J was faced with these two decisions: a decision of the House of Lords which appeared to hold that a photograph of a public figure (or any person, for that matter) engaged in day-to-day activities in public was not capable of grounding an application for breach of confidence absent some element which rendered the activity which was photographed 'private', and a decision of the European Court which appeared to hold otherwise.

Patten J noted that one of the difficulties about the European Court's judgment in *Von Hannover* is to 'identify and dissect from the Court's reasoning the precise factors which in its view engage the Princess's rights under Article 8'.[10] As already discussed above, for the most part, the photographs which were the subject of the claim were entirely innocuous.

While a broad reading of the decision in *Von Hannover* would suggest that a public figure had a legitimate expectation of not being photographed without consent on every occasion on which they were not on public business, Patten J took the view that a close reading of the judgments in *Von Hannover* suggested that a distinction could be drawn between a child (or an adult) engaged in family and sporting activities on the one hand, and something as simple as a walk down the street or a visit to the grocers on the other:

> *The first type of activity is clearly part of a person's private recreation time intended to be enjoyed in the company of family and friends. Publicity on the test deployed in Von Hannover is intrusive and can adversely affect the exercise of such activities. But if the law is such as to give every adult or child a legitimate expectation of not being photographed without consent on any occasion on which they are not, so to speak, on public business, then it will have created a right for most people for protection of their image. If a simple walk down the street qualifies for protection, then it is difficult to see what would not. For most people who are not public figures in the sense of being politicians or the like, there will be virtually no aspect of their life which cannot be characterised as private.* [11]

His Honour ultimately concluded that the Murrays' claim stood no reasonable prospects of success. This was because, firstly, there remained even after *Von Hannover* 'an area of innocuous conduct in a public place which does not raise a reasonable expectation of privacy',[12] and secondly, because 'even if the decision in *Von Hannover* has extended the scope of protection into areas that conflict with the principles and the decision in *Campbell*', Patten J was bound to follow *Campbell.*[13]

Finally, Patten J took some comfort from the fact that the case before him was 'indistinguishable' from the facts in *Hosking v Runting.*[14] In this case, the New Zealand Court of Appeal had recognised a tort of privacy but found that it was not available in respect of a photograph of the eighteen month old twins of well known parents being pushed down the street by their mother on the basis that the photographs revealed nothing sensitive or intimate in nature and were taken in a public place.[15]

The Court of Appeal

The Court of Appeal did not take issue with Patten J's statement of the relevant principles, nor his articulation of the appropriate test; namely did David Murray have a reasonable expectation of privacy when being pushed in his buggy and, if so, were the circumstances such that the Article 10 rights of the publisher ought to prevail over any right to privacy.

Patten J fell into error, according to the Court of Appeal, in his application of that test, and in particular in failing to distinguish between the position of a child and that of an adult when determining whether or not there was a reasonable expectation of privacy.

According to the Court of Appeal judges, it is at least arguable that children have a reasonable expectation of privacy in circumstances where an adult may not, and that David Murray – who had been completely unaware of a photograph being taken, let alone published - had a reasonable expectation not to be photographed.[16]

Perhaps surprisingly, given that this appears to have been the first occasion on which an English court has considered a fact scenario of this kind, the Court does not provide any detailed explanation of the basis for determining that children may have a reasonable expectation not to be photographed going about their day to day life in public. On the facts before the court in this case, there was no evidence of harm or inconvenience being caused to David (he was not aware that the photographs were taken or published). Nor was there any suggestion that the photographs had some potential to embarrass him at some later time when he was old enough to become aware of them.[17] Rather, the judges refer in fairly general terms to the 'rights of children' as recognised by the courts and the *United Nations Convention on the Rights of the Child* (to which the UK is a party)[18], and to the *Press Complaints Commission Editors' Code of Practice* (*the* ***Code***), which provides that editors must not use the fame, notoriety or position of the parent or guardian as sole justification for publishing the details of a child's private life.[19] While noting that a publication called *The Editors' Codebook* states that the *Press Complaints Commission* has ruled that the mere publication of a child's image cannot breach the Code when it is taken in a public place and unaccompanied by any private details or materials which might embarrass or inconvenience the child, the Court of Appeal judges state that 'it seems to us that everything must depend on the circumstances.' [20]

But *what* circumstances might be relevant to any consideration of whether a child had a reasonable expectation of privacy not to be photographed notwithstanding that the taking of the photograph causes no harm or inconvenience and the publication is not such as to embarrass the child?

The Court of Appeal refers, with apparent approval, to the following statement by the Press Complaints Commission in connection with a complaint made by former Prime Minister Tony Blair and his wife:

> *…the acid test to be applied by newspapers in writing about the children of public figures who are not famous in their own right (unlike the Royal Princes) is whether a newspaper would write such a story if it was about an ordinary person.* [21]

The Court suggests that such an approach is arguably appropriate to the question of whether the child of famous parents has a reasonable expectation of privacy with respect to innocuous *photographs* taken in public.

Does that mean that the child of a famous parent has a reasonable expectation of privacy *whenever* he or she is out and about in public? While the Court of Appeal suggests not, noting that 'there may well be circumstances in which there will be no reasonable expectation of privacy, even after *Von Hannover*',[22] the judges offer little assistance in determining where the line should be drawn. They reject as unhelpful the distinction suggested by Patten J between a child (or adult) engaged in family and sporting activities versus something as simple as walking down the street:

> *…an expedition to a café of the kind which occurred here seems to us to be at least arguably part of each member of the family's recreation time intended to be enjoyed by them and such that publicity of it is intrusive and such as to adversely affect such activities in the future. We do not share the predisposition identified by [Patten J] that routine acts such as a visit to the shop or a ride on a bus should not attract a reasonable expectation of privacy. All depends on the circumstances. The position of an adult may be very different from that of a child.* [23]

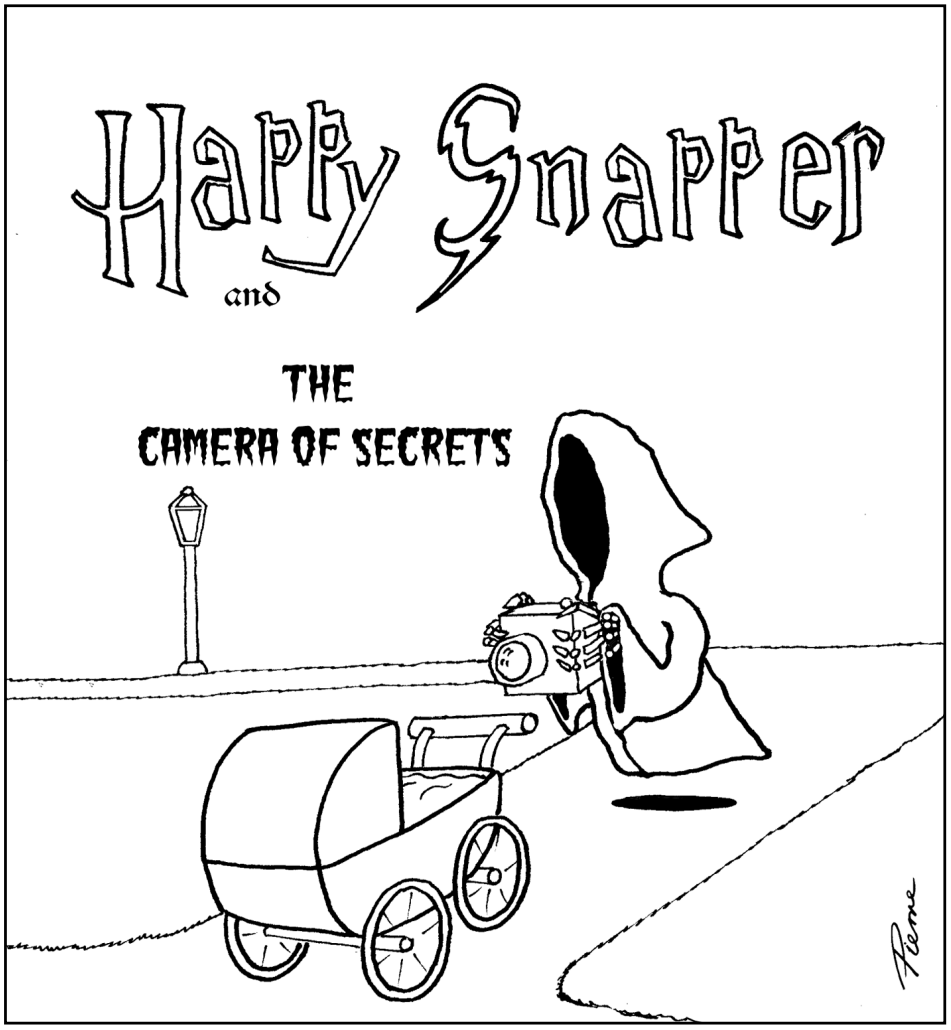
There is a suggestion by the Court of Appeal – not fully developed in their judgment – that the question whether or not the parent or guardian of the child would have objected to the photographs is somehow relevant to determining whether the child had a reasonable expectation of privacy:

> *It seems to us that, subject to the facts of the particular case, the law should indeed protect children from intrusive media attention, at any rate to the extent of holding that a child has a reasonable expectation that he or she will not be targeted in order to obtain photographs in a public place for publication which* ***the person who took or procured the taking of the photographs knew would be objected to on behalf of the child****. That is the context in which the photographs of David were taken.*[24]

The Court of Appeal judges seek to distinguish an earlier decision,[25] in which the court expressed doubt as to whether Article 8 was engaged in respect of the publication of a photograph taken in a Malta street of the survivor of conjoined twins, on the basis that the parents in that case would have permitted publication had they been able to agree a price with the newspaper. It is not altogether clear why the question whether a child has a reasonable expectation of privacy should be determined according to whether or not *his or her parents* had intended to commercially exploit media interest in the child, particularly given the Court's emphasis on the 'rights of children' and its insistence that the position of parents on the one hand and children on the other are distinct.

The Court of Appeal's willingness to draw a distinction based on whether or not the parents would have permitted publication (at a price) also appears to be at odds with its decision in *Douglas v Hello*.[26] It will be recalled that in that case, actors Michael Douglas and Catherine Zeta Jones were awarded damages for breach of confidence in respect of unauthorised publication in *Hello!* magazine of photographs of their wedding. Counsel for *Hello!* had submitted that the couple forfeited any entitlement to rely on what was essentially a breach of privacy claim when they agreed to sell photographs of their wedding. The Court of Appeal disagreed. The fact that their interest in seeking to control publication appeared to be largely commercial did not stand in the way of Douglas and Zeta Jones calling into aid their Article 8 rights in respect of a publication which they had not authorised.

It is to be hoped that when the Murrays' breach of privacy claim on behalf of their son is finally determined, the Court will explore in some greater detail than did the Court of Appeal the question of what factors, if any, justify treating children differently to adults when it comes to the question of their entitlement to go about their day to day life in public without being photographed.



Anne Flahvin is a Senior Associate in the Media and Content practice at Baker & McKenzie and teaches Media Law at UNSW.

(Endnotes)

1 [2008] EWCA 446

2 The Court of Appeal judges rejected the suggestion by Patten J, the judge who struck out the privacy claim, that to allow the claim would have been to introduce an image right. At paragraph 54, they note that Patten J had focussed his attention on the *taking* of the photograph, rather than on its publication. The Court of Appeal judged suggested that 'in the absence of distress or the like, the mere taking of a photograph in the street may well be entirely unobjectionable. We do not therefore accept, as the judge appears to suggest at paragraph 65, that, if the claimant succeeds in this action, the courts will have created an image right.' With respect, the distinction offered by the Court of Appeal judges between the mere taking of a photograph and its publication does not appear to be an answer to the suggestion that a successful claim on the facts as pleaded in Murrays' case will have effectively introduced an image right into English law, at least with respect to children.

3 [2007] EWHC 1908 (Ch)

4 [2004] 2 AC 457

5 Note 3 above, at para 96

6 Ibid, para 154

7 [2004] EMLR 21

8 Ibid, para 54

9 Ibid, paras 59-60

10 Note 2 above, para 43

11 Ibid, para 65

12 Ibid, para 68

13 Ibid

14 [2005] 1 NZLR 1

15 Note 2 above, paras 33 - 35

16 Ibid

17 It was factors of this kind which appear to have led the New Zealand Court of Appeal to determine in *Hosking v Runting* that 18 month old twins did not have a reasonable expectation not to be photographed while out in the public with their mother.

18 Ibid, para 45

19 Ibid, para 45

20 Ibid

21 Ibid, para 46

22 Ibid, para 55

23 Ibid, paras 55-56

24 Ibid, para 57

25 *MGN Ltd v Attard*, unreported decision of Connell J, 9 October 2001

26 [2005] EWCA Civ 595

European privacy laws a stumbling block for ASIC

Nick Hart looks at how European rights to privacy have recently dealt a blow to ASIC's requests in the UK to obtain information for its investigations in connection with the infamous Offset Alpine affair.

The Offset Alpine affair

The Offset Alpine affair has attracted much public attention and intrigue because of its mix of high-profile figures, large sums of money, and suspicions of criminality.

It began with the purchase from Kerry Packer of the Offset Alpine printing firm in 1992 and its subsequent flotation by the late Rene Rivkin, the flamboyant and successful stockbroker.

At the end of 1993 the firm's principal asset, the printing plant, was destroyed by fire. It transpired that the plant was valued at approximately $3million but had been insured for the replacement value of around $42million. A payout of over $50million caused the value of the company's shares to increase dramatically.

ASIC investigation

ASIC launched an investigation in 2003 into share trading at the company – following an investigation by the *Australian Financial Review* into the alleged secret ownership of a parcel of the shares in the company on behalf of Mr Rivkin, former minister Graham Richardson, and businessman Trevor Kennedy. It was alleged that Mr Rivkin and Mr Kennedy had used Swiss banks to hold the shares so that their beneficial ownership was kept secret and that perjury had been committed in evidence given to the Australian authorities.

Judicial review

The recent High Court proceedings in London were for judicial review brought personally by the Swiss lawyer, Benno Hafner, and his law firm Hafner And Hochstrasser, who acted for all three men connected with the affair. The defendant in this case was a lower English Court that had ruled previously that the information sought by the Australian Securities and Investments Commission (**ASIC**) did not concern any rights to privacy under European law.

The chain of events leading to these most recent proceedings began in late 2004 when the Attorney General requested on ASIC's behalf that the UK authorities assist it in obtaining evidence from the UK under the *UK Crime (International Co-Operation) Act 2003* (**CICA Act**).

The request for information sought the taking of evidence from two employees in London of Mees Pierson Intertrust Ltd (**MPI**), including questions regarding the connection between this company and the Swiss lawyer, Benno Hafner.

Claim for breach of privacy

Both Mr Hafner and his law firm had concerns that the information sought by ASIC included private correspondence and professional correspondence subject to Swiss confidentiality laws and legal professional privilege. Their claim was that any disclosure of this information would breach their privacy rights under Article 8 of the European Convention on Human Rights.

Interestingly, the information sought for disclosure did not only concern the men investigated by ASIC, but also information about Mr Hafner himself and particularly a document showing the beneficial shareholding interests of a number of individuals in various companies.

Prior to these recent proceedings, in 2006 the UK courts had already established a set of possible procedures which would give Mr Hafner and his firm opportunities to challenge disclosure sought by ASIC. These orders included the right for Hafner and his firm (the claimants) to appear and be legally represented, for the MPI employees to answer in writing a series of questions, and for counsel to make oral submissions to the court in determining whether the documents were relevant for disclosure under the CICA Act - but also whether they were 'inappropriate' for disclosure in light of the claimants' Article 8 privacy rights.

The procedure was agreed between ASIC and the claimants - but it was a permissive order rather than obligatory. As it happened, in subsequent hearings in London regarding the disclosure information sought by ASIC, the Judge of those hearings decided **not** to follow the agreed procedure. Instead, that Judge considered documents from Mr Hafner and his firm against disclosure, and a questionnaire in relation to the documents. On 27 March 2007 the Judge gave his decision about the disclosure, which included a somewhat surprising statement that the Article 8 privacy rights are not relevant – that 'Article 8 is not engaged in any way, shape or form'.

Judge 'manifestly in error'

It was on the basis of this statement about privacy that Mr Hafner and his firm made their claim – that the Judge had been 'manifestly in error' in deciding that their privacy rights are not engaged 'in any way, shape or form'. This was claimed not only in relation to the document of various beneficial shareholdings but also in relation to various documents that emanated from Mr Hafner and his firm and contained confidential information in relation to their clients.

The European rights to privacy

Article 8 of the European Convention on Human Rights, the 'Right to respect for private and family life', states:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The High Court's findings – privacy engaged

The High Court disagreed with the previous Judge that Article 8/privacy rights were 'not engaged'. In fact, the High Court stated that 'there can be no doubt' that compulsorily acquiring documents and information which were given by MPI to Mr Hafner and his firm in confidence – and then communicating that to a third party (ASIC) – engages the Article 8 privacy rights.

The High Court went on to confirm that it agreed with the following, which had been argued for Mr Hafner and his firm:

- That the protection of 'private life' and 'correspondence' can also include business correspondence;
- That even though Mr Hafner and his firm were not initially concerned in the legal proceedings, they were still given the protection of Article 8;
- That public authorities obtaining documents compulsorily must engage the right to respect for private life and correspondence in each step of obtaining, storing and using that information.

Safeguards against abuse

The lawyers for Mr Hafner and his firm cited various cases from the European Court of Human Rights in Strasbourg. This included the case *Franke v France (1993)* and this interesting extract from that judgment regarding foreign borders and privacy in connection with capital outflows and tax evasion:

> *'States encounter serious difficulties owing to the scale and the complexity of banking systems and financial channels and to the immense scope for international investment, made all the easier by the relative porousness of national borders. The Court therefore recognises that they may consider it necessary to have recourse to measures such as house searches and seizures in order to obtain physical evidence of exchange-control offences and, where appropriate, to prosecute those responsible. Nevertheless, the relevant legislation and practice must afford adequate and effective safeguards against abuse…'*

In this case, the safeguards were contained in the nomination of a court under the CICA Act to receive evidence and for judicial review proceedings. The High Court confirmed that when considering evidence, such a court would have to consider the privacy rights under Article 8 as well as legal professional privilege. This would apply regarding any person whose rights may be infringed if the application for the disclosure of evidence is granted.

The High Court stated that where prevention of crime is at stake then the rights to private and family life are unlikely to prevail – but that 'the court should protect documents or information that go beyond that which is necessary for this purpose'.

ASIC should have realised the Judge's error

The High Court referred the matter of assessing whether the documents and information should be disclosed back to a lower court – with the effect that the ASIC investigation will be further significantly delayed.

The High Court also accepted the arguments against ASIC that it should have been 'quite plain' that the original Judge had been wrong in his findings, and that even though judicial review would have been a necessary step to rectify that error, if ASIC had not opposed the judicial review it would have been a much shorter and less expensive process. The Court therefore ordered ASIC to pay two thirds of Mr Hafner and his firm's costs since the date of the previous order of 27 March 2007.

This can only add to ASIC's frustrations and illustrates that relying on possibly 'bad judgments' is not without risk.

Nick Hart is a lawyer at Truman Hoyle in the media, IP and technology group .

Communications & Media Law Association Incorporated

The Communications and Media Law Association (**CAMLA**) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the tele-communications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & on-line services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

Contributions & Comments

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in hard copy and electronic format and comments should be forwarded to:

Page Henty
C/- AUSTAR Entertainment Pty Ltd
Wilcox Mofflin Building
46-52 Mountain Street
ULTIMO NSW 2007
Tel: +61 2 9295 0153
Fax: +61 2 9295 0163
Email: phenty@austar.com.au

Matt Vitins
C/- Allens Arthur Robinson
Deutsche Bank Place
Corner Hunter & Phillip Streets
SYDNEY NSW 2000
Tel: +612 9230 4000
Fax: +612 9230 5333
email: matt.vitins@aar.com.au

Lesley Hitchens
C/- Faculty of Law,
University of Technology Sydney
PO Box 123
BROADWAY NSW 2007
Tel: +61 2 9514 3694
Fax: +61 2 9514 3400
Email: lesley.hitchens@uts.edu.au

CAMLA Website

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

Application for Membership

To: The Secretary, CAMLA, Box 545, Glebe NSW 2037
Tel/Fax: +61 2 9660 1645

Name:.....

Address: .....

Telephone: .....Fax: .....Email: .....

Principal areas of interest: .....

.....

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ I Ordinary membership $130.00 (includes GST)

☐ Student membership $45.00 (includes GST)
(please provide photocopy of student card - fulltime undergraduate students only)

☐ Corporate membership $525.00 (includes GST)
(list names of individuals, maximum of 5)

☐ Subscription without membership $150.00 (includes GST)
(library subscribers may obtain extra copies for $10.00 each + GST and handling)

Signature: .....