

PRIVACY

LAW BULLETIN

Volume 2 Number 1

Print Post Approved 243459/00067

Multi-layered privacy notices — a better way

contents

1	Multi-layered privacy notices — a better way
5	Cybersnooping employers to fall under the gaze of NSW laws
7	English Court of Appeal advances protection of private information
11	Privacy and the employee records exemption: a case of 'employer beware'
13	Privacy and the press
14	Eye spy privacy news

Information contained in this newsletter
is current as at May/June 2005

Marty Abrams CENTER FOR INFORMATION POLICY LEADERSHIP
and **Malcolm Crompton** INFORMATION INTEGRITY SOLUTIONS

Privacy notices are the windows to how organisations collect, use, share and protect the information that pertains to individuals. As information processes have become more complex, privacy notices have become very long, mirroring this complexity. The effect has been to obscure the content that individuals need to know when making judgments about with whom they will do business. The lack of clarity has been an impediment to online commerce.

This article describes a framework for assuring that notices are easy both to understand and follow as well as to complete. These objectives are achieved by layering up to three documents as part of a notices package. This approach, supported by an ad hoc group of civic, business and government participants, has been adopted by the European Union's Art 29 working party in Opinion WP100, issued in 2004. The initial layer, to be used when collecting information where space is tight, alerts the individual to the collection, the major purpose of the collection, and where they can go for additional information. The second layer, condensed notices, assist the individual in understanding a company's practices and comparing them to other companies' practices, while the third layer, longer notice, acts as a complete guide for compliance purposes.

We start this article with a brief review of the Australian legal context as set out in the National Privacy Principles (NPPs) that apply to private sector organisations in Australia under the *Privacy Act 1988* (Cth) and the APEC Data Privacy Framework adopted by APEC Ministers in November 2004.¹

It is our belief that multi-layered notices will help educate consumers in APEC economies (including Australia) as to how information that pertains to them is managed.

APEC privacy framework notice principle

The APEC privacy framework includes a notice principle that states:

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information ...

A successful privacy notice is a prerequisite for all privacy regimes. To align notices with the international standard, the principle states that a compliant privacy notice should include:

- the fact that personal information is being collected;
- the purpose for which personal information is collected;
- the types of persons or organisations to whom personal information may be disclosed;
- the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; and
- the choices and means that the personal information controller offers individuals for limiting the use and disclosure of, as well as accessing and correcting, their personal information.



Editorial board



Justice Michael Kirby
High Court of Australia

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

Siobhan Jenner
*Deputy Director, Compliance,
Office of the Federal Privacy
Commissioner*

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

Yee Fen Lim
*Associate Professor,
Department of Law,
Macquarie University*

Catherine Parr
Partner, Allens Arthur Robinson

Katherine Sainty
Partner, Allens Arthur Robinson

Narelle Smythe
Partner, Clayton Utz

Gayle Hill
Special Counsel, Freehills

Privacy Act's NPP notice principle

NPP 1.3² has a similar requirement, namely: 'At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of' a series of basic elements about who is collecting the information, the purpose of the collection, and with whom the information will be shared.

Current notices often too complex

Privacy authorities worldwide have found current privacy notices to be less than successful. Privacy notices were a focus of the 25th International Data Protection Conference held in Sydney in 2003, and were noted in the European Commission's review of the implementation of the EU privacy directive. The acting US Comptroller of the Currency (regulator of national banks) made notices the subject of her speech given on 12 January 2005. These authorities believe that the current privacy notices are often too long and complex, and that individuals often do not have knowledge about information practices after reading these long notices. Independent research by Yankelovich,³ 'Privacy & American Business'⁴ and others supports these findings.

Information processes tend to be very complex, and the descriptions of how information is collected, used, shared and protected often match the complexity of the subject matter. An analogy might be helpful. Think about the system of waterways that not only drain a geography, but also support agriculture, transportation, fisheries, power generation and recreation. Try describing the path a raindrop follows in making its way from the drainage ditch to a stream, creek, river and finally the sea. It would be hard to write a description in a very short, easy to read document, especially if one wanted to describe all the potential uses and users that might touch that drop.

Similarly, information that pertains to us is personal and its potential uses

complex, yet we want some sense of what is going on. With this in mind, in 2001 the Center for Information Policy Leadership (CIPL) in the USA and its member companies began work on making privacy notices more effective for individuals with the aim of enhancing public trust and participation.

Lessons from food label research

CIPL first looked at the research conducted in the 1980s to inform the creation of nutritional food labels. That research tells us the following.

- Notices must be short. Consumers get lost if presented with too much information. Notices should therefore discuss no more than seven discrete topics.
- Notices must use language that is so common that individuals are not required to translate what they read into what they understand. The words must be those that they use with their neighbours.
- Notices must rely on long and short term memories working together. The notice seen yesterday must help consumers understand the notices they see today. A common format that makes use of a common graphic interface accomplishes this objective. The research suggests a privacy notice that is easily recognisable as a privacy notice; is in a common format so individuals may easily find the information important to them; is in everyday language; and is short, having limited elements.

Using layering to accomplish readability and completeness

To fully define a complex organisation's information practices a notice must also be complete. How does one reconcile completeness with something that is short and easy to read and understand? Increasingly, organisations find that the answer lies in multi-layers. A multi-layered notice has two or more layers that work together to give the individual complete information in a manner in which one can understand information use and make choices. Layered notices were first suggested by CIPL in December 2001 at a workshop sponsored by US

financial services regulatory agencies. This approach became the subject of a resolution adopted by international data protection commissioners in September 2003,⁵ and was further refined by a March 2004 workshop that included government, civic society and business interests. The conclusions from that workshop were captured in the ‘Berlin Memorandum’.⁶ The ‘Article 29 Committee’ of data protection commissioners from the 25 EU Member States adopted this approach on 7 December 2004.⁷

The European data protection authorities suggest a notices system comprised of three layers:

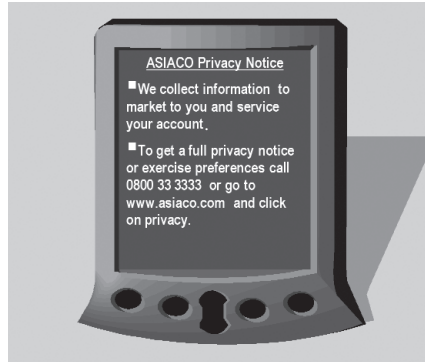
- short notice — detailing the party collecting information, the principal purpose, and where to go for more information and choices;
- condensed notice — a snapshot of an organisation’s information practices in a common, graphic format; and
- full notice — all information required by data protection laws or codes of conduct.

The short notice would be used when collecting information where space is an issue, like a mobile phone. On a PDA, for example, it might look like Example 1.

CIPL has developed a basic template for the condensed notice that was used in the examples included with the EU common position, and that is currently in use at a number of websites.

The condensed notice can be used on websites or in hard copy for off-line transactions. The complete notice would be provided on request, could be hyperlinked online, and would include:

- scope — the parties covered by the notice;
- personal information — information collected directly from the individual and from third parties;
- uses and sharing — a summary of uses by the organisation collecting the information and others;
- choices — the choices that individuals have, to limit sharing and gain access to the information held by the organisation, and how to exercise those choices;
- contacts — how to reach the organisation for the more complete notice; and



Example 1. A mobile phone displaying a short notice.

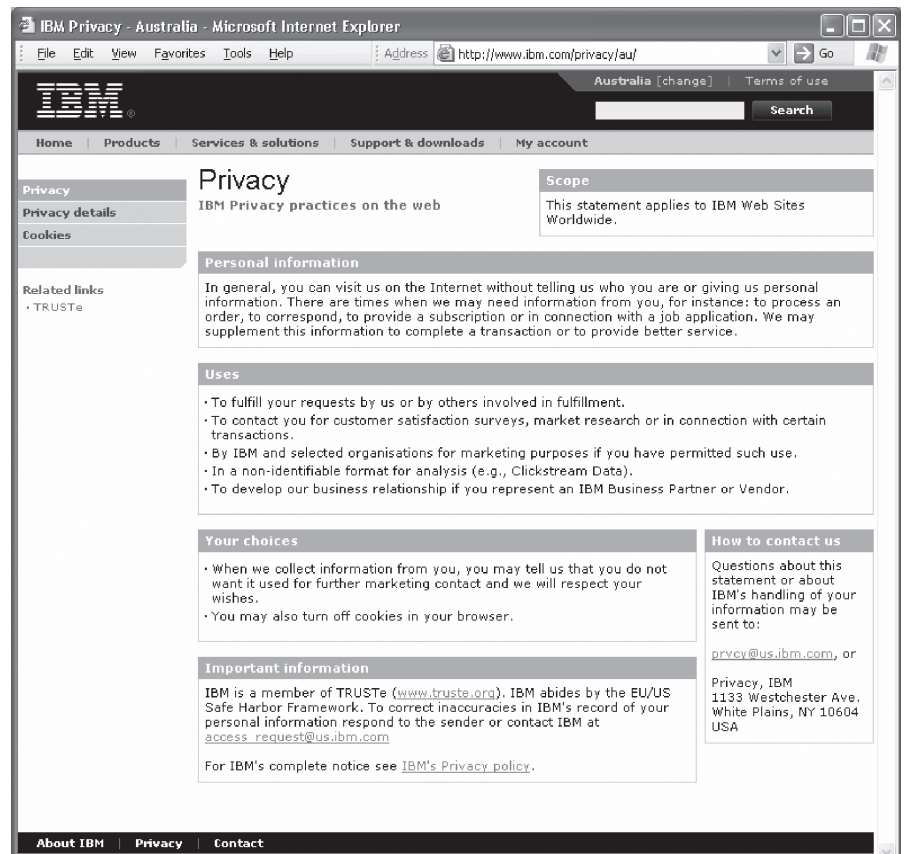
- other important information — information important to the individual, including seal programs⁸ and other systems for accountability. These categories are flexible enough to cover all the notice categories suggested by notice requirements such as those in the APEC privacy framework or the NPPs.

Major global companies are already posting notices in this format. The most notable is IBM, which has its condensed notice in this format for every one of its home page sites in every language it uses. See for example the privacy notice linked from <www.ibm.com/au>,

<www.ibm.com/cn> or <www.ibm.com/fr>. Other examples include MSN, in most languages, and, in Australia, Ninemsn at <www.ninemsn.com.au> and <www.pg.com>.

The IBM condensed notice looks like Example 2.

The advantage of multi-layered notices is that a single document is not being asked to achieve multiple objectives. The short notice notifies the consumer that information is being collected. The condensed notice gives the individual a snapshot of an organisation’s information practices, the options available to that person, and means of exercising those options. The complete notice defines purpose limitations and provides complete information on the organisation’s information practices. Importantly, as noted earlier, the notice also provides links to more detailed information. The condensed notice must facilitate, not hinder, the individual who wants to read and understand the full notice. The total package communicates clearly while being complete. Compliance would be determined not by a single



Example 2. IBM’s condensed notice.



element, but rather by the total package.

Focus group testing

The template based notices have been tested with focus groups in the US, Germany and Hong Kong. The US research was led by P&G and conducted in Cincinnati, Ohio. That research, conducted over two years (2002–03), found that consumers:

- believed that long notices were obscuring important information; and
- preferred a template that allows them to compare the practices of different companies.

The research in Germany and Hong Kong was conducted by MSN in 2004. That research determined that Hong Kong residents are too busy to read long notices, and therefore prefer the shorter, more graphically interesting template based condensed notice. Germans feel compelled to read long notices, but find them too long and complex. They too prefer the template based notice.

Where are we now?

The Privacy Commissioner only a few weeks ago repeated the endorsement of multi-layered notices in her report on the review of the private sector provisions of the *Privacy Act*, titled 'Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988' (the Review).⁹ In particular, in recommendations 19–20 she recommends that:

19. The Australian Government should consider amending NPP 5.1 to provide for short form privacy notices. This could also clarify the obligations on organisations to provide notice, and to clarify the links between NPP 1.3 and NPP 5.1.
20. The Office will encourage the development of short form privacy notices. It will also play a more active role in assisting businesses to develop their notices by developing template notices for different sectors, in consultation with them, and by issuing examples of both satisfactory and unsatisfactory notices.

Submissions to the Review,¹⁰ including from the Law Council of

Australia, also supported short form notices.

The privacy working group of the Electronic Commerce Sub-Group of APEC was again very supportive of multi-layered notices when it met in Hong Kong on 3 June 2005, and the concept was seen as a very practical early step by participants in the first implementation seminar held in the previous two days and attended by over 80 participants from 15 of the APEC economies.

IBM has published the IBM XML Asset Package for Privacy Notice Highlights v.1 as free assistance to businesses wanting to help create, translate and manage their privacy highlights document as an XML document. It is available online at <www.ibm.com/webmaster/news/privacynoticehighlights.html>.

Now is the time for business to take up the challenge. Regulators worldwide have repeatedly endorsed the multi-layered notice as good practice. Improved communications with customers can only win (not lose) business. There is undoubtedly first mover advantage in any one market such as financial services, or the components in it such as financial advice or retirement savings products. Assistance in implementing these notices is already available and the Privacy Commissioner has indicated that her Office will endeavour to provide more. ●

Marty Abrams is the Executive Director of the Center for Information Policy Leadership. Details are available online at <www.hunton.com/Resources/Sites/general.aspx?id=45>.

Malcolm Crompton is the Managing Director of Information Integrity Solutions, and was Federal Privacy

Commissioner until 2004. Details are available online at <www.IISpartners.com>.

Endnotes

1. 'APEC Ministers Endorse the APEC Privacy Framework', Media Release, Santiago Chile, 20 November 2004 at <www.apec.org/apec/news__media/2004_media_releases/201104_apecminsendorse_privacyfrmwk.html>.
2. See <www.privacy.gov.au/publications/npps01.html#a>.
3. 'A crisis of confidence: rebuilding the bonds of trust', presented to 10th Annual Customer Relationship Management Conference 2–4 June 2004 by Craig Wood, President, Monitor, Yankelovich Inc <www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State_of_Consumer_Trust_Report_-_Final_for_Distribution.pdf>.
4. See <www.pandab.org>.
5. See <www.privacyconference2003.org/resolution.asp>.
6. See <www.hunton.com/files/tbl_s47Details/FileUpload265/681/Berlin_Workshop_Memorandum_4.04.pdf>.
7. 'Opinion on More Harmonised Information Provisions', adopted November 2004 at <www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm>.
8. For an explanation of web seals, see Crompton M and Cavoukian A 'Web Seals: A review of Online Privacy Programs' at <www.privacy.gov.au/publications/seals.html>; see also <www.truste.org>.
9. Available online at <www.privacy.gov.au/act/review/index.html>.
10. All are available online at <www.privacy.gov.au/act/review/reviewsub.html>.

website

For the latest up to date information on new product titles, existing business and legal publications, ordering online and much more, contact us at: www.lexisnexis.com.au

Cybersnooping employers to fall under the gaze of NSW laws

Maree Norton, Andrew Cardell-Ree and Julian Riekert ALLENS ARTHUR ROBINSON

Workplace surveillance in NSW is about to change, and change significantly. If the Workplace Surveillance Bill 2005 (NSW) becomes law, employers will be permitted to conduct 'cybersnooping' activities only in accordance with a published computer monitoring policy of which employees are made aware. A failure to notify employees of surveillance plans in this way will constitute an offence, unless the employer first obtains the express authority of a magistrate.

Draft exposure Bill released in 2004

Existing workplace surveillance laws in NSW¹ regulate how an employer can use video cameras to conduct surveillance of its employees, but do not apply to surveillance conducted using computers or tracking devices. In June 2004, a draft exposure Workplace Surveillance Bill (the Draft Bill) was introduced to the NSW Parliament, proposing to regulate all manners of surveillance in the workplace (including email and computer use). The extension of the regulatory regime to cover computer surveillance is particularly controversial, given that such surveillance is common in Australian workplaces.² At the time of its release, NSW Attorney-General, Mr Bob Debus, said that the Draft Bill would not place a blanket ban on email surveillance, but would instead force employers to carry out email surveillance 'ethically and sensibly' and prevent 'unscrupulous employers snooping into the private emails of workers'.³

Following a period of consultation with major stakeholders, a revised Workplace Surveillance Bill (the Bill) was tabled in the NSW Parliament on 4 May 2005. The Legislative Review Committee has not identified any issues with the Bill, which is expected to become law in early June 2005.

Employees, workers and volunteers 'at work'

The Bill regulates surveillance 'at work', which includes surveillance conducted at an employer's usual place of business and

at any other place where an employee, volunteer or person engaged through a labour hire arrangement performs work on behalf of another (including the vehicle of a person whose work involves driving). If passed into law, the Bill will affect all entities that monitor the work activities of individuals in NSW.

The presumption of unlawful surveillance

The Bill proposes to extend the existing video surveillance regime to all forms of surveillance in the workplace, including surveillance of email and internet use and the use of tracking devices, such as global positioning systems. In short, the Bill presumes that surveillance is unlawful unless it is conducted in one of two sets of circumstances, as set out below.

Overt surveillance

Overt (or 'notified') surveillance will be lawful in NSW without further authority only if an employer provides employees with at least 14 days' written notice of the surveillance before it begins.⁴ Such notice must include details about the surveillance such as:

- the kind to be carried out (camera, computer or tracking);
- how it will be carried out;
- when it will start;
- whether it will be continuous or intermittent; and
- whether it will be for a specified limited period, or ongoing.

The Bill also imposes the following specific notice requirements, depending on the nature of the proposed surveillance.

- As is the current case, video surveillance and security cameras must be clearly visible and accompanied by signs notifying people that they may be under surveillance in the relevant area.⁵ Such signs must be situated at all access points to the area under surveillance.
- Computer surveillance must be carried out in accordance with the employer's computer surveillance policy and (in

language sure to be the subject of litigation) the affected employee must have been notified of that policy beforehand 'in such a way that it is reasonable to assume that the employee is aware of and understands the policy'.⁶

- Tracking surveillance must be accompanied by a notice informing occupants that the movements of the vehicle are subject to surveillance.⁷ Again, such signs must be clearly visible on the vehicle.

Any surveillance that does not meet *all* the requirements of notified surveillance is deemed to be covert surveillance, which is unlawful without the approval of a magistrate.

Covert surveillance

To conduct covert surveillance lawfully, an employer must first obtain from a magistrate a 'covert surveillance authority' (an Authority). A magistrate cannot grant an Authority unless the employer demonstrates a reasonable suspicion that an employee is involved in an unlawful activity while at work.⁸ The employer must also set out the steps that have already been taken in an attempt to detect the unlawful activity.⁹ Any covert surveillance must be conducted for the sole purpose of establishing involvement in unlawful activity and must be overseen by a court appointed 'surveillance supervisor'.¹⁰ Covert surveillance must not be undertaken to monitor work performance.

The Bill does not consider the meaning of 'unlawful activity'. Under the existing workplace video surveillance laws upon which the Bill is based, breach of an employer's policy does not amount to unlawful activity, and hence is not a sufficient basis for the granting of an Authority. There is no suggestion that the position will change if the Bill is made into law.

Offences and personal liability

Employers who conduct surveillance without either meeting the notified



surveillance requirements or obtaining an Authority are deemed to have engaged in unlawful activity, and may be subject to fines of up to \$5500 per offence. A defence is available only if the covert surveillance was carried out for the purpose of ensuring workplace security in circumstances where there was a real and significant threat, and the employer notified employees in writing of the intended surveillance in advance.¹¹

Directors and others involved in the management of a company are taken to have committed an offence if they knowingly authorised or permitted the contravention. Such individuals may be personally convicted even if proceedings have not been brought against the company.¹²

Other aspects of the regime

The Bill prevents automatic blocking of emails or access to websites, including the blocking of emails and websites 'merely' because they promote or relate to industrial matters.¹³

Implications — policies and procedures

If the Bill is passed in its current form, all employers who do business in NSW will need to formulate carefully worded policies and procedures to meet the requirements of notified surveillance. In his Second Reading speech, the NSW Attorney-General stated that the notice requirements were 'not onerous'.¹⁴ Despite this, the requirement that employees who are subject to computer surveillance be notified of the employer's policy 'in such a way that it is reasonable to assume that the employee is aware of and understands the policy'¹⁵ is uncertain, and likely to be the subject of litigation. The Bill does not give any indication of what this requirement entails, although Mr Debus has hinted at the sorts of notice systems that might satisfy the requirements:

An example of such a system for a large employer is one including induction and training courses and regularly emailed reminders. An example for a small business is individual discussion of the employer's policy with each employee and placing the policy on a work noticeboard.¹⁶

While the Draft Bill suggested that live, on-screen, pop-up reminders might have been a requirement of notified computer surveillance, much criticism was levelled at the practicability of that suggestion, which has subsequently been left out of the revised Bill.

Implications — relying on evidence of wrongdoing?

The Bill sets out two circumstances in which information gathered as a result of unlawful surveillance may still be relied upon.

- Where covert surveillance is conducted without an Authority, the information collected may only be disclosed to a member or officer of a law enforcement agency for a purpose that is related to the detection, investigation or prosecution of an 'offence'.¹⁷
- Information obtained in circumstances where the cl 21 defence¹⁸ is available can only be admitted in evidence in disciplinary or other legal proceedings against an employee where the desirability of admitting the evidence outweighs the undesirability of admitting evidence obtained unlawfully.

Otherwise, the Bill generally prevents employers who engage in unlawful surveillance from relying on evidence of wrongdoing that the surveillance uncovers, with potentially far reaching consequences for employers.

Consider the example of an employee dismissed for storing material on the employer's computer system that is deemed to be inappropriate by a policy which was not notified to the employee. If the employee claims unfair dismissal and the Industrial Relations Commission finds that the absence of training means that the employer's computer monitoring does not amount to notified computer surveillance, what then? If the employer cannot rely on the surveillance results, how can it establish the misconduct or a valid reason for the dismissal?

What if the wrongdoing was discovered as the result of routine surveillance that the employer conducted without an Authority in circumstances where no defence is available? Will an employer be able to rely on the results of such surveillance in

defending an unfair dismissal claim?

The reference in cl 36(3) to 'law enforcement agency' suggests that the use of the term 'offence' in that clause refers to a criminal offence. Consequently, the exceptions allowing reliance upon unlawfully obtained surveillance material in that clause may not apply in relation to a breach of an employer's internet policy, for example.

The only hope for employers in such circumstances may be to argue that the term 'surveillance' contains a temporal element, meaning that information gathered through 'after the event' interrogation of a computer hard drive may not be caught by the Bill. Beyond this, it seems that employers in NSW will have little choice but to comply with the notified and authorised surveillance regimes once the Bill is passed. ●

Maree Norton, Lawyer, Andrew Cardell-Ree, Senior Associate, and Julian Riekert, Partner, Allens Arthur Robinson.

Endnotes

1. *Workplace Video Surveillance Act 1999* (NSW).
2. *The Australian* newspaper recently reported that 30 per cent of employers with staff of over 100 are estimated to monitor the content of employee email activity (*The Australian* 5 May 2005).
3. Address to the Legislative Assembly, Question without Notice, 23 June 2004 at <www.parliament.nsw.gov.au/prod/parlament/hansart.nsf/V3Key/LA20040623026>.
4. The relevant notice requirements are set out in Pt 2 of the Bill.
5. Clause 11.
6. Clause 12.
7. Clause 13.
8. Clause 22.
9. Above note 8.
10. Clauses 19, 26 and 28.
11. Clause 21.
12. Clause 42.
13. Clause 17(4).
14. Second Reading Speech, *Workplace Surveillance Bill*, Extract from NSW Legislative Assembly Hansard and Papers, Wednesday, 4 May 2005.
15. Clause 12.
16. Above note 14.
17. Clause 36(3).
18. Above note 11.

English Court of Appeal advances protection of private information

Tony Wilson FREEHILLS

In what has been described as a ‘landmark’¹ decision, *Michael Douglas, Catherine Zeta-Jones v Hello Ltd*,² the England and Wales Court of Appeal on 18 May 2005 took a significant step forward in the development of what has been called the tort of misuse of private information.

There were a number of appeals and cross appeals from the decision of the trial judge on the merits of the Douglasses’ claim for the protection of commercial confidentiality and privacy in relation to photographs taken at their wedding. This article focuses on the significant outcome: the dismissal of the appeal by *Hello!* magazine against the trial judge’s finding in favour of the Douglasses and the underlying reasons for that decision.

The decision reflects the rapid development of the recognition of a basis for aspects of privacy protection in England during the period beginning with the decision of a differently constituted Court of Appeal³ to discharge the interlocutory injunction granted against the publication of unauthorised photographs taken at the Douglasses’ wedding, until the 2005 decision. In the meantime, according to the Court of Appeal, the decision of the House of Lords in *Campbell v MGN*⁴ and the European Court of Human Rights’ decision in *von Hannover v Germany*⁵ had advanced the recognition of privacy⁶ to the extent that, if the earlier Court of Appeal had considered those decisions, ‘it would have reached the conclusion that the Douglasses appeared to have a virtually unanswerable case for contending that publication of the unauthorised photographs would infringe their privacy’.⁷

The Court also dealt with a number of other issues with commercial implications for celebrity figures and the media which are dealt with briefly

after discussion of the central privacy issue.

Facts

The Douglasses married at the Plaza Hotel New York on 18 November 2000. There was intense media interest. In the UK, *Hello!* and *OK!* magazines provide gossip and rumour about royalty and celebrities, predominantly through photographs, with an average weekly circulation of almost 500,000 copies each.

After approaches by both magazines, the Douglasses entered into a contract with *OK!* for a combined fee of £1,000,000. *OK!* was granted exclusive rights to publish photographs selected and approved by the Douglasses. There was also agreement about security to ensure privacy, and sophisticated measures were taken to ensure that family and friends who were invited to the wedding were properly identified. Despite all the precautions, a paparazzo obtained entry to the wedding reception and surreptitiously took photographs.

When the Douglasses and *OK!* magazine became aware that *Hello!* had obtained unauthorised photographs of the wedding and was preparing to publish them, an ex parte application for an interlocutory injunction was made and granted. On appeal to the Court of Appeal two days later, the interlocutory injunction was lifted.

Both magazines then proceeded to publish within days of one another, respectively, the unauthorised and authorised photographs.

The trial of the actions brought by the Douglasses and *OK!* magazine subsequently commenced and a judgment on liability issues was given on 11 April 2003.

The trial judge’s findings

The trial judge found that:

- the Douglasses were entitled to

damages and a perpetual injunction against *Hello!* in the jurisdiction on the basis that the publication of the unauthorised photographs constituted a breach of confidence, effectively because the reception was a private event;

- *OK!* was entitled to damages from *Hello!* on substantially similar grounds where the breach of confidence was more in the nature of a trade secret; and
- the economic torts of deliberate interference with business or conspiracy to injure, either by lawful or by unlawful means, were not available to *OK!* against *Hello!*.

The trial judge rejected the Douglasses’ argument that damages should be calculated on the basis of a notional licence fee and awarded them £3750 each for the distress caused by the publication of the unauthorised photographs, and £7000 between them for the cost and inconvenience of having to hurriedly select authorised photographs to be published in *OK!*, so as to narrow the gap between that publication and the slightly earlier publication in *Hello!*. *OK!* was awarded £1,026,706 as its loss of profit from the exploitation of the authorised photographs and a small sum in respect of wasted costs.

The trial judge was hesitant about whether the Douglasses could base their claim on a separate head of privacy, saying that the law of confidence provided them with an adequate remedy, and if it did not then Parliament should act to fill the gap.

The appeals

There were appeals and cross appeals against the trial judge’s decision by most parties. *Hello!* challenged the trial judge’s decision that the Douglasses were entitled to relief on the basis either of breach of confidence or a right to privacy, and *OK!*’s right to damages. The Douglasses



appealed against the amount of damages awarded to them and the rejection of the notional fee basis for their damages.

The Court of Appeal, in a unanimous judgment delivered by Lord Phillips MR, summarised the trial judge's findings on the central issue. His Honour had noted the stimulation of the development of actions for breach of confidence and privacy following the introduction of the *Human Rights Act 1998* (UK). His Honour also concluded that breach of confidence rights can be shared with others where appropriate; in this case, shared with *OK!* as a result of the exclusive licence agreement.

The trial judge described the basis of the Douglases' case as 'one of either commercial confidence or of a hybrid kind in which, by reason of it having become a commodity, elements that would otherwise have been merely private became commercial'. The Court of Appeal agreed, saying that the Douglases' claim was based on invasion of their privacy and damage to the commercial interests in exploiting that private information. The grant of the exclusive licence to *OK!* was designed to preserve a residual confidentiality or privacy in relation to the wedding.

Hello!'s arguments on appeal

On appeal, *Hello!* argued that the trial judge's approach, in finding a hybrid right, was incorrect. The Douglases had a personal right in the nature of a privacy right which would be infringed by publication of photographs of the wedding only if that publication would be 'highly offensive to a reasonable person'. Further, it was a non-transferable right which was lost when transferred to *OK!*. It was also argued that once the photographs were published by *OK!* any privacy rights ceased because that publication placed the photographic information in the public domain. Then a further argument was put that any damages assessed should reflect the values protected by the relevant legal principle, that is to say, privacy values, and not be assessed on the basis of confidential information.

A rapidly developing area of English law

The Court of Appeal agreed that the *Human Rights Act* had acted as a catalyst for the development of privacy rights by importing the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (the Convention) into English domestic law. The judgment notes that when the legislation was introduced into Parliament it was made clear that judges would develop law protecting privacy, having regard to the requirements of the Convention.

An important question about the impact of the Convention had been asked by the author of a 'lucid article': does the Convention require states to provide a privacy remedy?⁸ That question was answered by the decision in *von Hannover v Germany*, a complaint brought by Princess Caroline of Monaco about published photographs in German magazines taken of her engaged in 'private' activities in public places. In that decision the European Court of Human Rights recognised an obligation on Member States to protect individuals from unjustified invasions of private life by other individuals or organisations, if necessary, by enacting legislation.

In subsequent English decisions, as noted by Lord Phillips MR, the courts had not been prepared to give the *Human Rights Act* 'full, direct, horizontal effect'.⁹ His Honour quoted Lord Nicholls in *Campbell v MGN* to the effect that, in England, 'unlike the United States of America, there is no over-arching, all-embracing, cause of action for "invasion of privacy"'.¹⁰

It is in that part of his judgment in *Campbell v MGN* that Lord Nicholls went on to describe the adaptation of the law of breach of confidence to one aspect of invasion of privacy, the wrongful disclosure of private information, as the tort of misuse of private information.

The impact of the Human Rights Act

Lord Phillips MR concluded, on the basis of his discussion of the impact of the *Human Rights Act*, that 'insofar as private information is concerned, we

are required to adopt, as the vehicle for performing such duty as falls on the Courts in relation to Convention rights, the cause of action formerly described as breach of confidence'. While that required the Court to give effect to Art 8 and 10 rights as set out in the Convention, and to have regard to relevant decisions by the European Court of Human Rights, particularly when considering what information should be protected as private under Art 8, his Honour noted:

We cannot pretend that we find it satisfactory to be required to shoehorn within the cause of action of breach of confidence claims for publication of unauthorised photographs of a private occasion.¹¹

The law of confidence

The Court of Appeal's judgment outlines the development of the law of confidence in England from *Albert v Strange*¹² onwards, and in particular its application to 'private' photographic information.

As recently as 1991, photographs of a celebrity in a hospital bed recovering from a serious head injury, taken as a result of unauthorised access by journalists, could not be protected by the law of confidence.¹³

But some four years later, as noted by Lord Phillips MR, Laws J made the following obiter comments:

If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment, as surely amount to a breach of confidence as if he had found or stolen a letter or diary in which the act was recounted and proceeded to publish it.¹⁴

When the earlier and differently constituted Court of Appeal came to consider the discharge of the interlocutory injunction in November 2000 it was, according to Lord Phillips, the first time a detailed analysis of the effect of the *Human Rights Act* on the protection of privacy had been carried out by an English court.

While the impact of the *Human Rights Act* had certainly developed the action in breach of confidence beyond the commercial and employment

relationships with which it was historically concerned, the Court of Appeal ‘discharged the injunction on the basis that the *OK!* contract had substantially weakened the Douglasses’ claim to relief based on invasion of privacy and that damages or an account of profits was likely to provide an adequate remedy should breach of duty be established at the trial’.¹⁵

The basis of the Douglasses’ privacy right

The Court of Appeal agreed with the findings of the trial judge that:

- the wedding was intended to be a private occasion;
- photographs were surreptitiously taken with the knowledge that the person taking them was not invited and not welcome; and
- those responsible for purchasing the photographs for publication in *Hello!* were aware that taking them involved ‘at least a trespass or some deceit or misrepresentation on the photographer’s part’.

The applicable test from the House of Lords decision in *Campbell v MGN* was as follows:

What the House was agreed upon was that the knowledge, actual or imputed, that information is private will normally impose on anyone publishing that information the duty to justify what, in the absence of justification, will be a wrongful invasion of privacy.¹⁶

The Court of Appeal also noted that in applying the test, both Arts 8 and 10 of the Convention are engaged: there is no presumption that an initial balance is made in favour of freedom of expression under Art 10.

Hello!’s argument that the law of New York, the place of the wedding, should be taken into account was rejected. The publication of the unauthorised photographs took place in England. The Douglasses’ claim for invasion of privacy was therefore to be determined according to the English law of confidence.

Hello! also argued that once the Douglasses had entered into the exclusive licence with *OK!* with a view to publishing authorised photographs, they could no longer claim that the

events of their wedding were private or confidential. While agreeing that this may in some cases be an accurate statement, the judgment notes that the publication of photographs could be distinguished from the publication of other personal information about a person’s private life.

In the latter case, once the information has been published there may be no useful purpose in prohibiting further publication. But in the case of photographs, the Court of Appeal made a number of separate points:

- photographs convey more than information and intrude on privacy by focusing on intimate personal detail;
- there will be a fresh intrusion of privacy when each additional viewer sees an ‘objectionable’ photograph;
- photographs portray, not necessarily accurately, personality and mood;
- authorising the publication of selected photographs would not reasonably exclude an individual’s right to be distressed about the publication of unauthorised photographs taken on the same occasion; and
- ‘[t]he objection to the publication of unauthorised photographs taken on a private occasion ... is that they disclose information that is private’.¹⁷

The fact that the Douglasses entered into an exclusive licence with *OK!* did not negate their claim that the wedding was a private occasion. By extending the law of confidence in this way, individuals whose private life is a valuable commodity are able to manage publicity as part of their trade or profession. Information about a celebrity is therefore a trade secret, and granting an injunction against publication of such information or damages rests on the commercial damage caused by the infringement of the monopoly right to make such private information public.

The recognition of this right of celebrity, according to the Court of Appeal, broke new ground. It was analogous to the protection of trade secrets in equity where they had been divulged in breach of a confidential relationship.

Based on the authorities it referred to, the Court of Appeal concluded that they reflect the following principles:

Where an individual (the owner) has at his disposal information which he has created or which is private or personal and to which he can properly deny access to third parties, and he reasonably intends to profit commercially by using or publishing that information, then a third party who is, or ought to be, aware of these matters and who has knowingly obtained the information without authority, will be in breach of duty if he uses or publishes the information to the detriment of the owner.¹⁸

The right created — non-proprietary and non-transferable

The Court of Appeal overruled the trial judge’s decision that *OK!* was also entitled to damages in relation to the publication of the unauthorised photographs by *Hello!*. Private information in such circumstances cannot be treated as property that can be owned and transferred. As a consequence, *OK!* only had an exclusive licence to exploit the photographs commercially for a nine month period.

The unauthorised photographs invaded the privacy which the Douglasses had chosen to retain by selecting and authorising the publication of certain photographs. The Douglasses had the right to protect this area of privacy or confidentiality. The Douglasses’ right to protect their private information through legal action did not extend to *OK!*. In any case, the licence agreement expressly retained all rights not expressly granted by the Douglasses to *OK!*.

OK! has announced that it will seek leave to appeal to the House of Lords on the issue of its entitlement to damages for loss of profits.

Claim based on economic torts

OK! argued its case for damages alternatively on the basis of what are known as the economic torts. While it is not the intention to discuss that area



of the claim in this article, the Court of Appeal agreed with the trial judge that a claim based on them failed, ultimately because *OK!* could not establish *Hello!*'s intention to inflict economic harm on *OK!*.

The Australian position

Although there do not appear to be any decided cases on point, surveillance devices legislation in Australian States and Territories would appear to provide protection against unauthorised photographs in situations like that of the Douglasses' wedding. For instance, the WA *Surveillance Devices Act 1998* creates criminal penalties for the installation, use or maintenance of optical surveillance devices and the publication or communication of a record of a private activity.¹⁹ The penalty for individuals is \$5000 or imprisonment for 12 months, and for body corporates, \$50,000.

The *Surveillance Devices Act 1999* (Vic) and the *Surveillance Devices Act 2000* (NT) contain similar provisions to the WA Act. The Surveillance Devices Bill 2004 (Cth) is currently before Federal Parliament.

Permanent injunctive relief would no doubt issue on proof of the elements of these offences. Further, in those Australian States and Territories which have enacted surveillance devices legislation, the established prohibition against publication would apply without the need for a court to undertake a balancing test like that required in England as a result of the protection of freedom of expression in Art 10 of the Convention.

Conclusion

Although the Court of Appeal's decision will attract critical comments from those, like Jonathan Morgan, who argue that until Parliament 'grasps the nettle' and recognises the 'direct horizontal effect' of the Convention in English domestic law 'so ensuring the full protection of human rights', there should be 'a bold and open engagement with the questions by the courts'.²⁰

Indeed, as noted above, the Court of Appeal was not comfortable with 'shoe horned' claims in relation to the publication of unauthorised photographs of private occasions into

the cause of action for breach of confidence. But, at the same time, the judgment makes clear that English law has moved forward in the protection of privacy. The Douglasses had 'a very strong claim'; one which may quite well have been 'clear enough to justify summary judgment in their favour', and one which was clearly a case for the issue of permanent injunctive relief.

Nevertheless, the Court of Appeal's clear and unambiguous finding that the primary remedy for an appropriate breach of the tort of misuse of private information is permanent injunctive relief will encourage plaintiff public figures that their privacy is protectable and deter efforts by the English media to publish unauthorised photographs of public figures in private situations.

The shaping of a right of privacy in English law based on Art 8 of the Convention will produce further layers of complexity. In an article²¹ written after the decision in *Campbell v MGN*, Mark Warby QC comments that privacy broadly protects not only the misuse of private information but also rights of autonomy and self-determination. In the case of celebrities he notes:

So long as the public is not misled or harmed, it may be asked why the famous should not be entitled to exercise their human right to self-determination by picking and choosing which aspects of their lives they show to the public [emphasis in original].

It has been recently reported²² that another forthcoming celebrity marriage between Peter Andre and Kate 'Jordan' Price is the subject of an exclusive arrangement with *OK!* for the sum of £2,000,000. The report notes that the agreement depends on no wedding pictures being published before their appearance in *OK!*, and further that Price and Andre will safeguard the agreement (and their fee) by hiring former SAS soldiers to ensure that there are no unwanted, unauthorised photographs.

Following the Court of Appeal's decision in favour of the Douglasses, the celebrity couple known as 'Dosh and Pecs' are in a much better position to keep their private information private and to protect their wedding day windfall fee. ●

Tony Wilson, *Special Counsel, Freehills.*

Endnotes

1. At the website of 5RB, 'a leading set of London barristers specialising in all areas of media and entertainment law, defamation and freedom of information' <www.5rb.co.uk>.

2. [2005] EWCA Civ 595.

3. *Douglas v Hello! Ltd* [2001] QB 967.

4. [2004] 2 WLR 1232.

5. ECtHR 59320/00, 24 June 2004 [2004] EMLR 379.

6. See Wilson T 'Privacy protection for photographs of individuals taken in public places' (2004) 1(2) Priv LB 21, which discusses privacy developments in English courts up to the decision in *Campbell v MGN*.

7. Above note 2 at [253].

8. Phillipson G 'Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act' (2003) 66 MLR 726.

9. See Morgan J 'Privacy, confidence and horizontal effect: "Hello" trouble' (2003) CLJ 444, an article written after the first instance decision which is critical of the 'timorous' even 'intellectually dishonest' approach of English courts involved in the 'incremental development' of privacy law in England.

10. Above note 4 at [11].

11. Above note 2 at [53].

12. (1849) 1 Mac & G 25.

13. *Kaye v Robertson* (1991) 19 1PR 147.

14. *Hellewell v Chief Constable* [1995] 1 WLR 804, 807.

15. Above note 2 at [67].

16. Above note 2 at [82].

17. Above note 2 at [105]–[107].

18. At [118].

19. By reference to the definitions of 'optical surveillance device' and 'private activity'; and s 6 dealing with the regulation of the use, installation and maintenance of optical surveillance devices; and s 9, dealing with the prohibition against the publication or communication of private conversations or activities.

20. Above note 9 at 473.

21. 'Privacy law in transition' para 27 at 5RB website, see above note 1.

22. *The Sunday Times*, Perth WA, 29 May 2005, p 53.

Privacy and the employee records exemption: a case of ‘employer beware’

Karen Hasluck-Janes and Ante Golem FREEHILLS

The *Privacy Act 1988* (Cth) was amended in 2001 to regulate for the first time the way private sector organisations collect, use, keep secure and disclose personal information through the introduction of the National Privacy Principles (NPPs).¹ There was much debate both leading up to and following the passing of the amendments between those who considered that the *Privacy Act* did not go far enough to protect individuals from the misuse of their personal information and those who considered that the *Privacy Act* simply imposed another layer of administrative burden on private organisations, already drowning in increased administration as a result of GST, the other legislative newcomer.

Perhaps partly in response to this criticism, the Government introduced two key exemptions which exempt most small businesses and employee records from the operation of the *Privacy Act*. The employee record exemption was a particularly hard fought victory for opponents of the *Privacy Act*. In effect, the *Privacy Act* exempts an act or practice of an organisation, that is or was an employer of an individual, from the operation of the *Privacy Act* so far as the act or practice is directly related to a current or former employment relationship between the employer and the individual, and is an employee record held by the organisation and relating to the individual.

However, the employee record exemption has not been without criticism, such as from those who say it encourages employers to be lax with the way employee records are dealt with. In addition, there is a perception that the employee record exemption is not as all encompassing as some employers think, and that some employers may be breaching the *Privacy Act* by misusing employee records.

The recent decision of the New South

Wales Administrative Decisions Tribunal (NSWADT), *NW v NSW Fire Brigade*,² is an example of misuse of an employee record. While the decision considered the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) (the NSW Privacy Act), the case has implications for employers who are subject to the Privacy Act.

Facts of the case

NW worked for the Sutherland Shire Council (the Council). NW had received permission from the Council to serve as a firefighter with the NSW Fire Brigade (the Brigade). However, the Council became suspicious that NW was working for the Brigade on days when he had called in sick to work at the Council.

Following a number of absences, a manager at the Council sent a written request to the Brigade seeking details of NW's attendance at the Brigade in order to see if 'there is a correlation between [NW's] time off work [with the Council] and his obligations to the [Brigade]'.

On receiving the request, a human resources manager at the Brigade arranged to inspect the occurrence book. The occurrence book recorded matters such as calls for assistance and records of attendance for duty, including the names of officers attending. The manager compiled details of NW's attendance and sent an email containing the relevant information to the manager at the Council. Upon receiving the information, the Council conducted an investigation into NW's conduct and terminated NW's employment.

Relevant legislation

Following the termination, among other things, NW commenced an action against the Brigade for contravention of the NSW Privacy Act.³ The NSW Privacy Act sets standards for dealing with personal information and applies to NSW State and local government agencies. Relevantly, the

NSW Privacy Act provides that a 'public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency'.⁴

The NSW Privacy Act defines 'personal information' as:

information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.⁵

This definition of personal information is almost identical to the definition of personal information under the *Privacy Act*.

The decision

The Brigade relied on two grounds. First, that the conduct was not affected by the NSW Privacy Act because the information fell within the 'publicly available publication' exception.⁶ In the alternative it relied on its second ground: that the disclosure was permitted because it was covered by an exception to the general prohibition on disclosure of personal information.

The Brigade failed on its first ground, as it was found that the occurrence book was an internal administrative document.

Second, the Brigade relied on an exception created by the NSW Privacy Commissioner that a relevant agency need not comply with s 18 of the NSW Privacy Act if non-compliance is reasonably necessary for the proper exercise of any of the agency's investigative functions or its conduct of any lawful investigations (the Investigation Exception).⁷

After considering the proper construction of the exception and reviewing arguments in relation to the issue previously considered at first instance



and on appeal,⁸ the NSWADT found that the plain meaning of the Investigation Exception requires that the same agency must be performing the 'investigative functions' or conducting the 'lawful investigations'. Consequently, the Brigade contravened the NSW Privacy Act and breached NW's privacy when it disclosed personal information about NW derived from the occurrence book to the Council.

Wider implications

The decision in this case has implications both for organisations subject to the NSW Privacy Act and for employers who are subject to the *Privacy Act*. In this case, the NSWADT held that the Brigade was not entitled to rely on the Investigation Exemption because the use of the personal information was not for an investigation being conducted by the Brigade. Employers should not assume that the employee record exemption will protect them in respect of any use of employee records. This is clearly not the case, as can be seen from applying the principles in *NW v New South Wales Fire Brigades*.

If the decision in *NW v New South Wales Fire Brigades* had been decided in the context of the *Privacy Act*, the use and disclosure of NW's employee record by the Brigade would not have been directly related to NW's employment with the Brigade. Therefore the employee record exemption would not have been applicable. This may raise an issue for employers whose employees are employed or perform roles with other organisations. It might therefore be prudent for employers to ensure that, where employees hold other jobs or roles, the employee's contract of employment clearly provides for the exchange of information relating to the employee.

However, another area where this issue may raise concern is during the due diligence process for the sale and purchase of a business. It remains common practice during due diligence processes for vendors to disclose employee records and other personal information to prospective purchasers to allow the carrying out of due diligence investigations.

The Office of the Federal Privacy Commissioner has published an information sheet to assist organisations in this area.⁹ The information sheet

touches on a vendor's obligations when disclosing information about employees to a prospective purchaser. It provides:

Where the vendor organisation discloses personal information about employees, the disclosure will fall within the employee record exemption if the information disclosed directly relates to a current or former employment relationship between the employer and the individual and to the employee record held by the organisation. The disclosure must also relate directly to such employment relationship. Examples would be where the disclosure is necessary to enable the prospective purchaser to assess whether or not to employ particular individuals from the vendor organisation.

Following the decision in *NW v New South Wales Fire Brigades*, the issue is whether a disclosure of employee records by a vendor employer to a prospective purchaser to enable the prospective purchaser to assess whether or not to employ particular individuals is directly related to the employment relationship between the employee and the vendor. There is an argument that where the sale of a business is occurring by way of an asset sale, the disclosure of employee records by a vendor to enable a prospective purchaser to decide whether to employ particular individuals is not directly related to the employment relationship between the vendor and the employee. Arguably the disclosure is related to the prospective employment relationship between the prospective purchaser and the employee, and therefore neither vendor nor purchaser could rely on the employee record exemption.

Where a sale of business is occurring by way of a share sale, the disclosure of employee records by the vendor is arguably directly related to the employee's employment with the employer, and would therefore be covered by the employee record exemption. Prior to completion of the share sale however, prospective purchasers could not rely on the employee record exemption. In the information sheet, the Commissioner has stated that:

Since due diligence investigations must be conducted confidentially to protect the interests of the organisations involved, the Commissioner takes the view that, even if personal information is recorded by a

prospective purchaser, it would generally be reasonable at this time for the prospective organisation to take no steps under NPP 1.5 to advise the individual about whom personal information is collected of the NPP 1.3 matters. Taking no steps would only be reasonable where the prospective purchaser organisation decides not to proceed with the purchase of the business, and returns or destroys all records of personal information to the vendor organisation.¹⁰

The approach outlined by the Commissioner is a common sense approach and recognises the confidentiality which usually accompanies business acquisitions, especially in the early stages. However, NPP 1.5 provides:

If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

While NPP 1.5 contemplates exclusions from the obligations under NPP 1.3 in circumstances which would pose a serious threat to the life or health of any individual, there is no express exclusion for circumstances where a transaction may be subject to confidentiality obligations. In addition, it is not clear from the wording of NPP 1.5 that by virtue of the confidentiality obligations it is reasonable to take no steps in all cases. For these reasons, it would be prudent for both vendors and purchasers to consider only dealing with de-identified employee records, particularly in the early stages of a due diligence when confidentiality is most important. In addition, employers should consider including privacy clauses in employment contracts (particularly those of senior employees) which, among other things, could include a provision whereby the employee agrees to the disclosure of the employee's employment records to prospective purchasers of the business.

Conclusion

The decision in *NW v New South Wales Fire Brigades* has raised some interesting privacy issues for employers, not just in NSW but in Australia

generally. Employers should not assume that the employee record exemption in the *Privacy Act* is unrestricted and that all dealings with employee records will be subject to the exemption.

Given the success of the employee in *NW v New South Wales Fire Brigades*, employers may find that an increasing number of employees will attempt to pursue breaches of their privacy rights and test the limits of the employee record exemption under the *Privacy Act*. ●

Karen Hasluck-Janes, Senior Associate, and Ante Golem, Solicitor, Freehills.

Endnotes

1. See the *Privacy Amendment (Private Sector) Act 2000* (Cth).
2. [2005] NSWADT 73.
3. In NSW the invasion of privacy, including the misuse of personal information, is unlawful under various state and federal laws which include the *Privacy Act* and the NSW *Privacy Act*.
4. Section 18(1) of the NSW *Privacy Act*.
5. Section 4(1) of the NSW *Privacy Act*.
6. Section 4(3)(b) of the NSW *Privacy Act*.

7. *Direction on Processing of Personal Information by Public Sector Agencies in Relation to Their Investigative Functions*, NSW, 31 March 2003.

8. *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78 and then on appeal, *Vice-Chancellor, Macquarie University v FM* [2003] NSWADTAP 43.

9. Information Sheet 16 — Application of key NPPs to due diligence and completion when buying and selling a business, October 2002.

10. Above.

Privacy and the press

Professor Ken McKinnon AUSTRALIAN PRESS COUNCIL

Privacy issues will loom larger and larger for the press in future, both in Australia and elsewhere. The current patchwork of federal and State privacy laws in Australia, essentially limited to protection of personal tax file numbers, credit information, data matching and health information, is already under review. Growing concern about individual privacy is driving new legislative and judicial action.

It is doubtful, however, whether new action to protect individual privacy can be achieved without curtailing traditional press freedom. Recourse to the International Convention on Civil and Political Rights is no help in finding a balance. The Convention includes clauses proclaiming both the right of people to a free flow of information and their right to privacy, but no guidance on where the balance lies or any satisfactory means of resolving conflict. For countries like Australia, which has no constitutional protection of freedom of the press, the balance will very likely have to be forged in the heat of politics, unless, by default, the courts simply go their own way.

Dealing with complaints

Newspapers would say that privacy is already adequately regulated. Under the federal *Privacy Act 1988* (Cth) newspapers that publicly abide by a regulatory privacy code are exempt from direct regulation. Currently the Australian Press Council resolves any privacy

complaints about a newspaper from a member of the public (using Principle 3 of its Statement of Principles). Newspaper respect for such sanctions is demonstrated by the fact that fewer than 5 per cent of the complaints received each year by the Council are about invasion of privacy. In any case, the print press has well defined staff handbooks governing the ethics of privacy and publication.

Press surveillance restrictions?

One force driving stronger current attention to privacy is the increasing availability and lower cost of powerful surveillance devices that monitor movement, photograph participants, identify smells and monitor in other ways.

Proposals prepared by the NSW Law Reform Commission (the Commission) illustrate where change might lead. In its report the Commission recommended new laws to control surveillance, but in so doing sharply illustrated the problems. It defined surveillance as the use of a surveillance device where there is a deliberate intention to monitor a person, group, place or object for the purpose of obtaining information, whether overt or covert, whether in a public or a private place. The proposed definition could potentially include binoculars at sporting events or opera glasses at the theatre, the use of cameras in public places, and all web-cams, as well as a vast range of activities many of which would not be seen as remotely threatening to the

privacy of individuals. Moreover, there was a failure to define what constitutes monitoring and a lack of distinction between public and private.

If the Commission’s view prevails it would be necessary for a newspaper to seek approval for, or justify after the fact, any actions coming within the definition of monitoring to a court or bureaucrat. Almost any press activity in a public place might come within the scope of the proposed legislation, including photographing the crowd at a football match. The need to seek permission or justify actions later (including the requirement to report in writing to the Attorney-General and/or submit to searches by an inspecting authority) would certainly inhibit the ability of newspapers to carry out their role.

Recent WA surveillance devices legislation has created offences for installing, using or maintaining listening devices to record, monitor or listen to a private conversation, or optical devices to visually record or observe private activity, or to attach, install, use or maintain a tracking device to determine the geographic location of a person or object. It defines ‘private activity’ as excluding an activity the parties ought reasonably to expect may be observed; ‘private conversation’ is defined similarly. The *Surveillance Devices Act 1998* (WA) (the Act) includes provision for judge approved use of devices ‘in the public interest’. The Act has not caused



newspaper publishing problems to date, which is not to say it will not do so in the longer term.

Restrictive impact of court judgments

Although the UK Government has not so far moved on a 2003 proposal from the Commons Select Committee on Culture Media and Sport ‘firmly’ recommending that the Government should introduce statute law to clarify the protection that individuals can expect from invasion of their privacy, there has, nevertheless, been movement overseas towards institution of a tort of privacy via common law judgments. Notable cases that inch forward the existence of a tort of privacy, cases that are bound to affect court thinking in Australia, include *Douglas v Hello Ltd* (2003) (see article in this issue at p 7), the *Campbell v Mirror Group Newspapers* ([2002] All ER (D) 177) cases in the UK and the *Hosking v Runting* ([2005] 1 NZLR 1) case in NZ.

Grosse v Purvis

An important local decision was the judgment in *Grosse v Purvis* (2003) Aust Torts Reports 81-706, by the Queensland District Court in 2003. It established that it is possible to sue for breach of privacy in common law, that is, that there can be a civil action for damages based on the right of an individual to privacy. The case was decided in favour of the plaintiffs. Sizeable damages were awarded. Legal commentaries have been quick to note the implications of that decision for the media, claiming that journalists and media organisations that intrude offensively into people’s personal affairs may be exposed to actions for damages. As the judgment

was unrelated to the *Privacy Act*, the defences and exemptions in that Act cannot be relied upon, although a defence of public interest could be available in certain circumstances.

Conclusion

New legal jeopardy for newspapers is being developed in common law. Newspapers may also need to take account of a related judicial comment in the *Grosse v Purvis* case, to the effect that there could well be a tort of harassment, which would potentially have serious implications for the media.

It is too early to say definitively how far this trend will go, but it does appear that Australia is moving toward a tort of privacy. Until recently there has not been enough public discussion of privacy boundaries. The print press needs to consider what processes and approaches it thinks will be sufficient to protect a continuing free flow of information. The reference to the defendants having breached the Code of the Press Complaints Commission in the *Douglas v Hello Ltd* case may well be an element in consideration of desirable future developments.

If these threatened privacy rights become well established, how can the importance of the public interest, the public’s right to know, not be undermined? For instance, there are already suggestions that the publication of the image of a person or persons caught in a media melee outside a court might in future have to be subject to the explicit permission of the individuals involved. Could the press do their job if the outcome becomes one where individuals in the spotlight have the right to veto

publication of their images if unflattering, as in the case of a street theft, a dropped catch, or poor play?

Although no political party would dare put forward an agenda for directly limiting press freedom, in the absence of constitutional protection developments of the kind mentioned here they may just as effectively nibble away existing freedoms, particularly the right of the press to seek information if the potential public interest justifies persistent, detailed inquiries. Defamation law is already a big deterrent, resulting in court action by individuals to prevent information being published, even when it is clearly in the public interest for that information to be in the public domain. Careless extension of statute law, or over-enthusiastic judge-made common law, setting up a new privacy tort with ill defined parameters, could equally effectively hamper free speech.

Publishers, journalists and readers need to be aware of these developments and the possibilities for the emergence in Australia of restrictive privacy regimes with the undesirable and perhaps unexpected outcome of curtailment of free speech. The principles of privacy and freedom of expression inevitably collide in many circumstances. Action to protect private actions more effectively is understandable. But the reciprocal of protection of the historic right of the public to be informed on matters of public interest and concern is equally essential. Present trends suggest that there will not be sufficient open debate to shape a well considered balance. ●

*Professor Ken McKinnon,
Chairman, Australian Press Council.*

eye spy PRIVACY NEWS

Commissioner investigates health information disclosure

11 May 2005. ‘Most people consider that health information about them is quite sensitive. When my Office became aware that the personal information of patients may have been inappropriately

disclosed by doctors to CAMM Pacific via Health Communications Network Ltd’s (HCN) Medical Director software, I chose to investigate’, said Privacy Commissioner Karen Curtis.

‘The issue was brought to my attention by journalists, late last year, who alleged that CAMM Pacific and HCN were breaching the *Privacy Act*

1988 (Cth). At the time, CAMM Pacific was conducting a study which aimed at collecting data about the promotional activity sponsored by pharmaceutical companies.

‘CAMM Pacific received information via HCN who in turn received it from doctors via the Medical Director software that many of them were using.

‘It was also alleged that an extraction tool that removed information from the Medical Director software was faulty because it extracted the patient information of all doctors working in group practices, even those who had not elected to participate in the extraction exercise.

‘Following my Office’s investigation I have found that the patient information transferred from doctors to CAMM Pacific, via HCN’s Medical Director software, is de-identified and therefore does not fall within the definition of personal information outlined in the *Privacy Act*.

‘However, participating doctors are identified by CAMM and HCN on a consent based arrangement. I am satisfied that if a medical practice accidentally transfers the de-identified patient records of a non-consenting doctor that HCN cannot identify that doctor and does not use that de-identified patient information.

‘I have therefore concluded my investigations into CAMM Pacific and HCN and have found that that they have not breached the *Privacy Act*.

‘I’d like to acknowledge the co-operation my Office received from both CAMM Pacific and HCN during our investigations. Both organisations appear to take privacy seriously and are to be commended for this.

‘By law, health information is accorded a high level of privacy protection and if people have concerns that this may not be occurring they should contact my Office’, said Ms Curtis.

Source: <www.privacy.gov.au>.

Barbara Wellbery Memorial Award

13 May 2005. Individuals interested in privacy may wish to submit a paper to the Barbara Wellbery Memorial Award about privacy. Award winner(s) will receive \$US3000 in cash and the opportunity to present the paper to an international privacy conference in 2006.

As part of the Barbara Wellbery Memorial Award, a stipend of up to \$US2000 for associated travel expenses will also be granted and the paper will be published in the *International*

Review of Law, Computers & Technology.

The Award is open worldwide to individuals and co-writing partners, 18 years of age and older, from industry, law, government, academia and public interest groups, including students, and is granted annually by the Morrison & Foerster Foundation (MoFo Foundation). The deadline for entries is 1 October 2005.

Please download a copy of the application for further details: <www.privacy.gov.au/news/wellbery.pdf>.

Congress passes Real ID Act

16 May 2005. US Congress has passed a law that threatens to pave the way for a US identity card. The *Real ID Act*, which was tagged onto a military funding Bill, passed both the Senate and House of Representatives without full debate.

Source: <www.outlaw.com>.

Release of the report into the review of the private sector provisions of the Privacy Act

18 May 2005. Privacy Commissioner Karen Curtis welcomed the release by the Attorney-General, the Hon Philip Ruddock MP, of her report into the operation of the private sector provisions of the *Privacy Act* — ‘Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act 1988*’ (see <www.privacy.gov.au/act/review/index.html>).

‘This review is the first major examination of the private sector provisions in the *Privacy Act* since they commenced in December 2001’, said Ms Curtis.

‘While I have made a number of recommendations I believe that there is no fundamental flaw with the private sector provisions in the *Privacy Act*’, she said.

‘The overall effect is that the National Privacy Principles have worked well and delivered to individuals protection of personal and sensitive information in

Australia in those areas covered by the Act.

‘The Report has drawn on information and views from a wide range of sources including individuals, businesses, industry organisations, consumer representatives, and government agencies across the Commonwealth, States and Territories.

‘The review has benefited from discussions, consultations and suggestions made in submissions. I thank all those involved for contributing their ideas and views, and for the constructive way in which those views were conveyed.

‘The Report contains 85 recommendations stemming from a balanced and pragmatic examination of the *Privacy Act*, within the terms of reference set by the Attorney-General’, said Ms Curtis.

‘The recommendations in the Report relate to improving the operation of the private sector provisions and are written as actions the Australian Government should consider doing, or as measures the Office could undertake.

‘Of the 136 submissions my Office received, many organisations and consumer representatives agreed that to improve the privacy of all Australians it is important to ensure a nationally consistent privacy scheme.

‘The submissions also made it clear that the health sector would particularly benefit from national consistency and I have therefore recommended that a national health code be implemented across federal, State and Territory levels.

‘Another issue highlighted in many submissions was the need to raise the privacy awareness of organisations and individuals and therefore a number of my recommendations address this issue. Those recommendations, if implemented, would form the “lynch pin” of an improved privacy scheme that would benefit individuals while recognising the right of businesses to achieve their objectives in an efficient way.

‘Consumer control over personal information, a key feature of the private sector amendments to the *Privacy Act*, was addressed in the review. I have recommended that the control that individuals have over their personal

information be strengthened, particularly in relation to information collected about them indirectly or used or disclosed for other purposes such as direct marketing.

‘Simple steps that could be taken to make this happen include measures to promote clearer and more easily understood privacy notices and a general opt-out right for all direct marketing approaches.

‘The Report also contains recommendations about the small business exemption with the aim of simplifying its application while suggesting that some sectors that handle large volumes of personal information, such as internet service providers, should be covered by the private sector provisions.

‘Some recommendations in the Report relate to my Office and these include improving the transparency of the complaints process and to enable the Office to better identify and address systemic issues.

‘Because of their complexity, the issue of privacy and research, in particular medical research, and privacy and new technologies warrant further debate. The main recommendation on these issues is that they should be considered in the context of a wider review of the *Privacy Act*.

‘During the review, it became apparent that while the private sector provisions work well, it may be appropriate for the Government to undertake a wider review of

privacy for Australians in the 21st century.

‘Throughout the Report, but particularly in the recommendations, there has been careful consideration of the balance between protecting individual rights while recognising the collective needs of the community including the business community.

‘I look forward to the debate about the issues raised in the Report’, said Ms Curtis.

The Report is available at <www.privacy.gov.au/act/review/index.html>.

Source: <www.privacy.gov.au>.

Inaccurate reporting on health information

26 May 2005. Privacy Commissioner Karen Curtis has said ‘[r]ecent media reports about the Office’s investigations into information flows between doctors and the Health Communications Network Ltd (HCN) and CAMM Pacific are inaccurate and may have led to confusion among consumers’.

‘It is important that people know that I have not approved any deal between HCN and CAMM,’ said Ms Curtis.

‘Allegations were raised last year that those companies and some doctors could be breaching the *Privacy Act* and I chose to investigate. My Office’s role was to investigate the information flows between doctors, HCN and

CAMM and to apply the *Privacy Act* to those activities.

‘The *Privacy Act* applies to information where the identity of the individual is apparent, or can reasonably be ascertained, from the information. The Office is bound to make its decision about matters it investigates on the basis of the meaning of personal information as set out in the *Privacy Act*.

‘Following my Office’s investigation it was found that the identity of patients could not reasonably be ascertained. Therefore, the *Privacy Act* does not apply in the circumstances of this particular case.

‘There has been no change in the Office’s thinking on what constitutes personal information.

‘I have addressed the wider issues of the use of medical information for research purposes and the appropriateness of the definition of personal information in the *Privacy Act*, in my recent report on the Review of the Private Sector Provisions (released on 18 May 2005 and available at <www.privacy.gov.au/act/review/index.html>).

‘I have recommended that those issues should be subject to further discussion and debate to ensure that our privacy laws best serve the needs of all Australians. The Government will be responding to my recommendations’, said Ms Curtis. ●

Source: <www.privacy.gov.au>.

PUBLISHING EDITOR: Rob Macredie BA/LLB MANAGING EDITOR: Helen McKenzie MA PRODUCTION: Alex Mullan
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
TELEPHONE: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood www.lexisnexis.com.au rob.macredie@lexisnexis.com.au
ISSN 1449-8227 Print Post Approved PP 243459/00067

This newsletter may be cited as (2005) 2(1) Priv LB

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

Printed in Australia © 2005 Reed International Books Australia Pty Limited trading as LexisNexis ABN: 70 001 002 357

order form

Privacy Law Bulletin

I WISH TO PURCHASE

TITLE	NO OF COPIES	TOTAL
<input type="checkbox"/> A hardcopy subscription to <i>Privacy Law Bulletin</i> at \$563.20 per annum*		
<input type="checkbox"/> An electronic subscription to <i>Privacy Law Bulletin</i> at \$563.20 per annum**		
<input type="checkbox"/> Please contact me to discuss package and multi user options.		
	TOTAL \$	

*Yearly price is GST inclusive and includes 10 issues.

**Please note price for electronic format is based on one practitioner/user – please contact customer relations on 1800 100 161 for more details.

PERSONAL DETAILS

Mr/Mrs/Ms (Please circle)

First Name

Surname

Job title

Company name

Company address

Suburb State Postcode

Area of practice

Email

Telephone Fax

Signature

Date

(All orders must be signed for processing)

I Would Like To Pay (Please tick appropriate box)

Using my LexisNexis Account No: _____
If you do not have an existing LexisNexis account, please call 1800 100 161 to obtain a new account application form to send with this order. An account must be established in order to receive your updates.

Personal/Company cheque enclosed for \$_____ payable to LexisNexis

Bankcard Mastercard Visa Amex

Card Number: _____

Expiry Date: ___/___ Date: _____

Name on credit card: _____

Signature of cardholder: _____

SEND YOUR COMPLETED ORDER:

By Fax
1800 800 122

By Post
Order Management
LexisNexis
Locked Bag 2222
Chatswood Delivery Centre
CHATSWOOD NSW 2067

Freecall

1800 100 161 for further information or details on LexisNexis products and services.

TERMS AND CONDITIONS

*Price is in AUD and are current as of 20/06/05. Price is subject to change without notice and all orders remain valid until cancelled in writing. This offer is not valid in conjunction with any other offer and all are subject to acceptance by LexisNexis.

30-Day Guarantee

You have 30 days in which to examine any book or service published by LexisNexis Australia. If it fails to satisfy your needs, return it in saleable condition within 30 days of invoice and we will give you a full credit. No credit is given for books and services published outside Australia.

Important Privacy Notice

The information you provide on this form is being collected by Reed International Books Australia Pty Limited as LexisNexis Australia (LexisNexis) for the purpose of processing your registration or enquiry and keeping you informed of upcoming products, services offers and events. The information is disclosed from time to time to our related bodies corporate for these purposes. The provision of this information by you is voluntary but if you do not provide some or all of the requested information we may be unable to properly process your registration. You have both a right of access to the personal information we hold about you and to ask us to correct it if it is inaccurate or out of date. Please direct any queries to: The Privacy Officer, Reed International Books Australia or email to privacy@LexisNexis.com.au

I do not wish to be informed of LexisNexis product or services

©2005 Reed International Books Australia Pty Ltd trading as LexisNexis. LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc. and used under license. ABN 70 001 002 357