Communications LAW

B•U•L•L•E•T•I•N

E COMMUNICATIONS
CORPORATED

3/00011 EDITED BY NIRANJAN ARASARATNAM AND SHANE BARBER Vol 21 No 2 2002



124

# amation Law Reform on the Agenda Again: Proposed Reforms in New South Wales

**Sally Barber examines controversial proposals for changes to defamation laws**

The Carr Labor Government in New South Wales has foreshadowed reform to defamation law as one of the planks of its tort law reform program, which will be introduced by legislation in the Spring session of Parliament.

At a speech given at the Sydney Institute on 9 July 2002, Premier Carr referred to the complexity of defamation law and the high stakes involved in the protection of individual reputation resulting in long and expensive litigation and stated that the reforms are "about striking a balance between the community's right to know and protecting reputations". The Premier's stated view was that "too often damages awards for loss of reputation – non-economic loss – are excessive". He outlined a set of proposals including:

- making greater provision for resolution of disputes without litigation;
- detailing a process for the use of corrections and apologies, with costs penalties as an incentive, to settle claims and avoid litigation;
- reducing the limitation period for commencing proceedings from 6 years to 12 months;
- capping compensation for non-economic loss to the maximum amount allowed in personal injury cases, presently $350,000; and
- barring corporations and statutory bodies from bringing actions in defamation.

The Premier summed up by saying the proposed reforms *"will bring the same commonsense approach to defamation that we've brought to other areas involving civil damages"*[1] .

The proposals stem from a report by a task force on defamation law reform commissioned by the Attorney-General to overhaul the *Defamation Act 1974*, comprised of Professor Reg Graycar, New South Wales Law Reform Commissioner and Professor of Law at University of Sydney, Professor Ken McKinnon, Chairman of the Australian Press Council, Michael Sexton SC, New South Wales Solicitor General and Maureen Tangney, Director Legislation and Policy Division of the Attorney General's Department.[2]

## BACKGROUND

The *Defamation Act 1974* (NSW) (**Act**) last had significant amendments made to it in 1994.[3] Those amendments:

- limited the role of the jury in defamation trials to determining whether the pleaded imputations are conveyed by the matter complained of, and, if so, whether they are defamatory of the plaintiff (resulting in the advent of separate "section 7A jury trials" on meaning), with defences and damages to be determined by the judge alone; and
- made it a requirement that, in assessing damages, the trial judge is to take into consideration the general range of damages for non-economic loss in personal injury awards in NSW (including those regulated by statute).

## INSIDE THIS ISSUE

**Defamation law Reform on the Agenda Again: Proposed Reforms in New South Wales**

**The Media Ownership Bill - A Divided Senate**

**An Overview of New Zealand's New Telecommunications Regulatory Regime**

**Telstra Corporation Ltd. V Hurstville City Council Optus Vision Pty Ltd. V Warringah Council - The Decision of the Full Federal Court**

**Interception Law Under Scrutiny**

**Invasive Technology and Privacy Implications**

CONTENTS

**Defamation Law Reform on the Agenda Again: Proposed Reforms in New South Wales**
Sally Barber examines controversial proposals for changes to defamation laws

**The Media Ownership Bill - A Divided Senate**
Raani Costelloe provides an update on the cross media ownership debate.

**An Overview of New Zealand's New Telecommunications Regulatory Regime**
Seth Eeles examines New Zealand's new approach to telecommunications regulation.

**Telstra Corporation Ltd. V Hurstville City Council Optus Vision Pty Ltd. V Warringah Council - The Decision of the Full Federal Court**
Angela Brewer updates the progress of this watershed case regarding telecommunications infrastructure.

**Interception Law Under Scrutiny**
On the first anniversary of September 11, Ben Kuffer reviews the rise and fall of a key plank in the government's post September 11 2001 reforms.

**Invasive Technology and Privacy Implications**
Rebecca Sharman discusses the boundary of recent amendments to privacy laws when applied to new technologies.

## PROPOSALS AND COMMENTARY

In respect of the proposals foreshadowed by the Premier, reducing the limitation period for commencing proceedings is a sensible reform in circumstances where the object of defamation proceedings is restoration of the plaintiff's reputation. Arguably, the harm is immediate and so too should be the seeking of redress. The task force relied on this argument and empirical research showing that over 80% of actions are commenced within 6 months of publication in making its recommendation, which mirrors that of the NSWLRC's 1995 Report on Defamation.[4]

The recommendation for a cap on non-economic loss contrasts with the current position under section 46A of the Act, which is expressed as a guide only. It is not clear whether the statutory maximum is intended to apply to each imputation successfully found or to each proceeding overall[5], but a cap will increase certainty and make any cost benefit analysis regarding settlement options easier to undertake. However, the reality is that there have been very few awards by judges alone for non-economic loss which exceed $350,000[6], so that the cap may have little effect on damages awards.

There are many arguments for the proposal that the right to sue in defamation be limited to natural persons, including that other remedies are available to corporations for damage caused by a defamatory publication eg injurious falsehood, passing off and misleading or deceptive conduct under the *Trade Practices Act*, and that some corporations use the threat of defamation proceedings to silence critics[7] (see eg the "McLibel case"). Although section 65A of the *Trade Practices Act* prevents proceedings against media organisations under section 52 of that Act, section 52 can be a very effective alternative to defamation proceedings[8], particularly in respect of the availability of injunctive relief, especially where the defamatory publication is sourced from a competitor. Whilst Premier Carr's view is that corporations and statutory bodies can defend their reputations in the media and by "winning the public debate"[9], that argument only really applies to large corporations. Liability in defamation is often easier to establish than the alternative causes of action. For instance, proof of malice is required to establish injurious falsehood. Removal of the right to sue in defamation may therefore result in serious financial damage to a corporation, for which there is no remedy[10]. There are no good arguments for allowing statutory bodies to sue in defamation, given their role in society and the importance of citizens being able to speak freely about them.

The recommendations of the task force on defamation law reform, in addition to that which was foreshadowed by the Premier, involve the inclusion of a statement of objects and principles in the Act, including "to promote speedy and non-litigious methods of resolving disputes wherever possible"[11].

The recommendations also include a proposal for a new part in the Act called "Resolution of Disputes without Litigation" which will constitute the first substantive part of the Act and provide for a detailed process for corrections and apologies and, where appropriate, monetary compensation, to be available before proceedings are issued. It is not clear precisely how this process would be implemented and the extent to which it would be mandatory, but the report refers to "a clear statutory preference for a pre-trial, non-litigious process"[12]. There is much to be said for implementing such a process, particularly given that most plaintiffs sue to restore their reputations and not for damages[13].

The task force recommends that costs penalties (more onerous than simply costs following the event) should attach to unreasonable failure to resolve the matter (eg. for a plaintiff, not accepting an offer of correction or apology where the offer is considered to have been reasonable; for a defendant, not making such an offer where it seemed appropriate to do so)[14]. Whilst this seems an admirable proposal, the question of how a judge would interpret reasonableness of a party's refusal to settle arises.

The task force also recommended that it should be a defence (where an action proceeds to that stage) that an offer was made as soon as practicable, the defendant remained ready and willing to perform the terms of the offer, and the offer was reasonable in the circumstances[15]. Again, the success of

# The Communications And Media Law Association Incorporated (CAMLA)

PO Box 545 Glebe NSW 2037 Australia

## CAMLA

## *Essay Prize*

*The Communications and Media Law Association is holding an essay competition in 2002.*

**The purpose of the competition is:**

- to encourage high quality work in communications and media law courses; and
- to improve links between those studying and practising in the area.

**The prize will be given for:**

- a previously unpublished essay which is the original work of the author;
- an essay completed by a student enrolled in an undergraduate or postgraduate course, possibly as part of that course;
- an essay on a subject relating to communications or media law; and being
- an essay of 1,000-3,000 words. The 3,000 word limit (inclusive of all footnotes, annexures, attachments and bibliographies, etc) is not to be exceeded.

***A prize of $1,000 and a one year membership of CAMLA will be awarded to the winner.***

The winning essay, edited in consultation with the author, will be published in the Communications Law Bulletin.

The winning entry, to be selected by a panel of experienced communications and media law practitioners, is likely to demonstrate original research, analysis or ideas. The panel will not necessarily be seeking detailed works of scholarship.

***The award will be made at the annual CAMLA Christmas function.***

Only one essay per student may be submitted. Entries will be accepted by email or by post. Entries WILL NOT be accepted by fax. Entries submitted by post should include three (3) copies of the entry, typed well-spaced on A4 paper. The name, address, email, telephone and fax contacts and the tertiary institution and course in which the author is enrolled should be included on a separate, detachable sheet. Entries submitted by email should include the same details in a separate email from the entry. The author's name should not appear on the pages of the essay.

Entries should be submitted to:

Administrative Secretary, CAMLA, PO Box 545. GLEBE NSW 2037, Australia

Email: rosie@bigpond.net.au

**by Friday 1 November 2002**

Late entries will not be accepted.

this reform will depend on judges' interpretation of what is a reasonable offer.

It was recommended that where proceedings had been issued, mediation should be encouraged wherever possible as an aid to resolution of disputes, such mediation to be conducted by an outside dispute resolution process, and that a practice direction should contain a list of accredited/authorised mediators[16].

The task force also recommends amending the statutory defence of qualified privilege (section 22) to make it a defence which is workable for the media, rather than the toothless tiger it currently is in a media context. There is only one reported case where a mass media defendant has successfully been able to rely on that defence, and the case involved a very unusual set of circumstances[17]. The task force proposes that there be added to section 22 a list of factors the Courts are to consider when assessing reasonableness, the requirement to demonstrate which is currently the downfall of most media attempts to rely on the defence. The factors are as follows:

- the extent to which the subject matter is a matter of public interest;
- the extent to which the matter complained of concerns the performance of the public functions or activities of the plaintiff;
- the nature of the information;
- the seriousness of the imputations;
- the extent to which the matter distinguishes between proven facts, suspicions and third party allegations;
- the urgency of the publication of the matter;
- the sources of the information and the integrity of those sources;
- whether the matter complained of contained the gist of the plaintiff's side of the story and, if not, whether a reasonable attempt was made by the publisher to obtain and publish a response from the plaintiff; and
- any other steps taken to verify the information in the matter complained of[18].

The Australian Press Council further proposed that section 22 be amended by adding a phrase into the beginning of the section, so that it reads as follows: "In the determination of whether the conduct of the publisher is reasonable under Subsection (1) *in the light of the duty of the press to publish matters of public interest* the following matters are relevant", because the Council believes this addition would have the effect of drawing the judiciary's attention to the fact that newspapers have an obligation to keep readers informed and that judgments have to be made about how carefully and comprehensively the newspaper conducted its inquiries in the limited time available before publication[19]. This no doubt stems from the perception, at least by media defendants, that the test of reasonableness as currently applied by the Courts is unrealistically onerous.

Some members (2 out of 4) of the task force expressed concern that the proposed list to be added to section 22 might not be seen as moving sufficiently far enough away from the current approach ( and there is merit in that view) and propose therefore that, in relation to the discussion of political and government matters only, an additional provision in the following terms be inserted: "There is a defence of qualified privilege for a publication concerning government and political matters" and then makes a non-exhaustive list of what would constitute such matters[20].

The effect of such an amendment would be a statutory broadening of the common law qualified privilege defence in relation to publications concerning government and political matters, abolishing the requirement of reasonableness which has posed such a barrier to mass media reliance on any form of the qualified privilege defence[21].

Under the section of the report dealing with case management, the role of juries and the section 7A trial, the task force recommended that the plaintiff should be required to take the necessary steps to bring a matter on for trial and that there be a default process if no action is taken after 12 months, whereby the matter lapses and the action is struck out automatically (in contrast to Part 32A Supreme Court Rules). Where an action lapses for want of prosecution, the task force recommended that there should be no order for costs. However, the task force recommended that a defendant be able to apply for costs, in which event a plaintiff could also apply for the matter to be reinstated. Otherwise, the Court should have a discretion as to whether the plaintiff should be given leave to reinstate an application once it has lapsed[22].

The task force recommended that there should be no change to the current process under which the section 7A trial is heard by a judge with the jury, and the defences and damages hearing takes place separately before a judge alone. Professor McKinnon dissented on this point, in line with a widespread view held by media defendants that the section 7A trial process introduced by the 1994 amendments to the *Defamation Act* have increased the complexity and expense involved in defamation proceedings[23].

Broadening the defence of protected report by creating a specific statutorily conferred form of protection for publication of certain third party statements, because of a perceived (and, if reasonableness continues to be interpreted restrictively, real) risk that even the revised section 22 would not protect publishers in respect of reporting defamatory third party statements. This would be achieved by making amendments to sections 24 and 25 of the Act, by adding to the list of proceedings of public concern the subject of a protected report defence "proceedings of a press conference given by a public official with the authority of a government body or instrumentality (including a minister of the Crown)" and adding to the list of official and public documents and records the subject of a protected report defence "a press release issued by a public official with the authority of a government body or instrumentality (including a minister of the Crown)". That would reduce the number of defamation proceedings founded on re-publication by the media of proceedings of press conferences and press releases made by third parties, and relieve the media of the obligation to check the veracity of such third party statements prior to publication.

In closing, the task force expressed its view that the proposals set out in its report could form the basis for discussion with the States and Territories, with a view to a further attempt to bring about national reform (there have been many attempts by the Standing Committee of Attorneys General, dating back to 1980)[24]. The task force's view is that any such reform process should include a re-think by NSW of the rule that makes the imputation the cause of action in that state, the only state where that rule applies. There have been contrasting views expressed about this

proposal[25], but arguably the resulting requirement of precision, whilst potentially increasing the number of interlocutory proceedings, simplifies the jury trial on meaning.

The proposals were welcomed by some Attorneys General of other States[26].

## CONCLUSION

The focus of the review by the task force was stated to be to strike a balance between the free flow of information on matters of public interest and importance and the protection of individual reputations.

The detail of the government's proposals, in the form of a Defamation (Amendment) Bill, are yet to be seen, and no doubt intense lobbying by all interested parties is taking place. It is to be hoped any amendments implemented assist in achieving the balance sought by the task force's stated aims, which can only be of benefit to both plaintiffs and defendants.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Sally Barber is a Senior Associate in the Sydney office of PricewaterhouseCoopers Legal.***


1 "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002; Press Release issued by Premier Carr, 9 July 2002; "Carr moves to restrict payouts for defamation", S. Gibbs and J. Pearlman, The Sydney Morning Herald, 10 July 2002.

2 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.(i).

3 *Defamation (Amendment) Act 1994* (No 93).

4 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.12; NSWLRC Report 75 (1995) – Defamation: Recommendation 37, p.204.

5 "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002.

6 "Change for change's sake will not serve the defamed", R.Coleman, The Sydney Morning Herald, 15 July 2002.

7 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.13-14.

8 See eg *Re: FAI General Insurance Co Limited and RAIA Insurance Brokers Limited* (1992) 108 ALR 479.

9 "Carr moves to restrict payouts for defamation", S. Gibbs and J. Pearlman, The Sydney Morning Herald, 10 July 2002.

10 See comments of Peter Bartlett as reported in "Mixed reaction to NSW reform package", A. Crossland, The Australian Financial Review, 12 July 2002.

11 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.(i)).

12 Ibid, pp.(ii), 6); "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002.

13 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.3.

14 Ibid, p.(ii).

15 Ibid, p.(ii).

16 Ibid, p.(ii)).

17 Tobin & Sexton, Australian Defamation Law and Practice, 14,090.

18 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.(iv)-(v).

19 Ibid, p.(v).

20 Ibid, pp. (v)-(vi).

21 See, in relation to government and political matters *Lange v ABC* (1997) 189 CLR 520 at 574.

22 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.11-12.

23 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform pp.8-9; "Change for change's sake will not serve the defamed", R.Coleman, The Sydney Morning Herald, 15 July 2002; "Defamation reformer presses on", K. Marshall, The Australian Financial Review, 19 July 2002.

24 NSWLRC Discussion Paper 32 (1993) – Defamation, paras 1.10-1.18.

25 See eg "Justice Levine says defamation law is not working: 'The nonsense must end'", Gazette of Law & Journalism, 1 September 1999; NSWLRC Report 75 (1995) – Defamation, paras 4.2-4.6),

26 "Push for defamation law unity", K. Marshall, The Australian Financial Review, 12 July 2002; "NSW plan 'doesn't go far enough'", K. Marshall and "Attorneys-general face full agenda for two-day meeting", K. Towers, The Australian Financial Review, 19 July 2002. "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002; Press Release issued by Premier Carr, 9 July 2002; "Carr moves to restrict payouts for defamation", S. Gibbs and J. Pearlman, The Sydney Morning Herald, 10 July 2002).

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.(i).

26 *Defamation (Amendment) Act 1994* (No 93).

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.12; NSWLRC Report 75 (1995) – Defamation: Recommendation 37, p.204.

26 "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002.

26 "Change for change's sake will not serve the defamed", R.Coleman, The Sydney Morning Herald, 15 July 2002.

26 Defamation Law – Proposals for

Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.13-14.

26 See eg *Re: FAI General Insurance Co Limited and RAIA Insurance Brokers Limited* (1992) 108 ALR 479.

26 "Carr moves to restrict payouts for defamation", S. Gibbs and J. Pearlman, The Sydney Morning Herald, 10 July 2002.

26 See comments of Peter Bartlett as reported in "Mixed reaction to NSW reform package", A. Crossland, The Australian Financial Review, 12 July 2002.

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.(i)).

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform pp.(ii), 6); "Cost penalties: big stick in defamation reform plot", Gazette of Law & Journalism, 24 July 2002.

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, p.3.

26 Ibid, p.(ii).

26 Ibid, p.(ii).

26 Ibid, p.(ii)).

26 Tobin & Sexton, Australian Defamation Law and Practice, 14.090.

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.(iv)-(v).

26 Ibid, p.(v).

26 Ibid, pp. (v)-(vi).

26 See, in relation to government and political matters *Lange v ABC* (1997) 189 CLR 520 at 574.

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform, pp.11-12.

26 Defamation Law – Proposals for Reform in NSW: Report of Attorney-General's Task Force on Defamation Law Reform pp.8-9; "Change for change's sake will not serve the defamed", R.Coleman, The Sydney Morning Herald, 15 July 2002; "Defamation reformer presses on", K. Marshall, The Australian Financial Review, 19 July 2002.

26 NSWLRC Discussion Paper 32 (1993) – Defamation, paras 1.10-1.18.

26 See eg "Justice Levine says defamation law is not working: 'The nonsense must end'", Gazette of Law & Journalism, 1 September 1999; NSWLRC Report 75 (1995) – Defamation, paras 4.2-4.6),

26 "Push for defamation law unity", K. Marshall, The Australian Financial Review, 12 July 2002; "NSW plan 'doesn't go far enough'", K. Marshall and "Attorneys-general face full agenda for two-day meeting", K. Towers, The Australian Financial Review, 19 July 2002.

# The Media Ownership Bill – A Divided Senate

**Raani Costelloe provides an update on the cross media ownership debate.**

The Senate Environment, Communications, Information Technology and the Arts legislation committee (**Committee**) released its Report on the *Broadcasting Services Amendment (Media Ownership) Bill 2002* (**Bill**) on 19 June 2002. The Bill was introduced into Parliament in late March 2002 and was immediately referred to the Committee. The Committee invited submissions and held public hearings at which it heard from interested parties.

The Bill proposes to amend the *Broadcasting Services Act 1992* (**BSA**) by repealing media-specific foreign ownership restrictions and creating an exemption to the cross-media ownership restrictions which would permit a person or company controlling a commercial radio licence, a commercial television licence and/or a newspaper in the same licence area (each a **media operation**) provided that separate editorial processes are maintained between the individual media operations.

The Report is in two parts:

- one part being the view of Government Senators comprising the majority of the Committee which supports the Bill subject to some recommendations; and

- the other part being the dissenting view of the minority Committee members of the Australian Democrats and Australian Labor Party (**ALP**) which rejects the Bill and calls for a broader inquiry into the media industry.

The Bill therefore faces a difficult passage through the Senate given that the Government requires the support of members of opposition parties in the Senate to ensure that it is enacted, particularly the ALP and the Australian Democrats. While the ALP has indicated support for the repeal of media-specific foreign ownership restrictions while opposing the cross-media ownership amendments, the Government has said that it will only deal with foreign ownership and cross-media together in one package and not separately.

## CURRENT CROSS MEDIA & FOREIGN OWNERSHIP RESTRICTIONS

The BSA presently prevents any one person controlling more than one of the following in any geographic licence area:

- a commercial free-to-air television licence;

- a commercial radio licence; or

- a major newspaper.

The BSA contains specific foreign ownership restrictions with respect to free-to-air and pay television licences, including:

- **free-to-air television**: foreign persons must not be in a position to **control** a free-to-air television licence and the total of foreign interests must not exceed **20%**;

- **pay television**: foreign interests are limited to a **20%** company interest in a pay television licence for an individual and a **35%** company interest in aggregate.

A person is regarded to be in a position to exercise control of a licence, company or newspaper if the person has company interests exceeding **15%**. Company interests can be shareholding, voting, dividend or winding-up interests. The Australian Broadcasting Authority (**ABA**) may also have regard to other non-company interest factors in determining the issue of control.

In addition to the BSA, there are controls on foreign investment in the media under the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (**FATA**). In summary:

- **all media**: all **direct** (ie. non-portfolio) proposals by foreign interests to invest in the media sector irrespective of size are subject to prior approval under the Government's foreign investment policy on a **national interest** basis. Proposals involving **portfolio** share holdings of **5%** or more must also be approved;

- **newspapers**: the maximum permitted aggregate foreign (non-portfolio) interests in **national** and **metropolitan** newspapers is **30%**, with a **25%** limit on any single foreign shareholder. The aggregate non-portfolio limit for **provincial** and **suburban** newspapers is **50%**.

## ABOLITION OF MEDIA SPECIFIC FOREIGN OWNERSHIP RESTRICTIONS

The Bill proposes to **repeal the media-specific foreign ownership restrictions** in the BSA with the effect that all foreign ownership investment in media will be only subject to the general foreign ownership laws under FATA which take account of national interest concerns. The Government's rationale is that the current restrictions impede investment in Australia and that the repeal of the restrictions would result in a more competitive media sector.

### Cross-media ownership exemption certificates

The Bill does not propose to repeal the cross-media ownership restrictions. Instead, it creates a regime whereby an entity seeking to take control of a set of media operations (in circumstances where control would breach the BSA) may apply to the ABA for an **exemption certificate**. The holder of an exemption certificate will not be in breach of the cross-media rules provided that the conditions of the certificate are met.

The application must identify the set of operations currently controlled and proposed to be controlled, and include proposed organisational charts and editorial policies that show how each media operation will achieve **separate**:

- editorial policies;
- editorial decision-making; and
- editorial news management, news compilation processes, and news gathering and interpretation capabilities.

Provided that separation is maintained in these areas, the relevant media operations may share resources and co-operate.

The rationale behind the exemption certificate regime is that it protects diversity of news sources and opinions while allowing for common control of media operations.

The ABA must issue an exemption certificate if it is satisfied that the conditions included in the application are sufficiently specific and detailed to meet the objective of editorial separation for the relevant set of media operations.

The observance of the objectives is a condition of the entity's relevant commercial television or radio broadcasting licence. The ABA's enforcement powers include notification of a licensee to rectify a breach and the suspension or cancellation of a licence.

### Regional news

The Bill also provides for new licence conditions on regional commercial television and radio broadcasting licensees which are subject to an exemption certificate to **maintain existing or minimum levels of local news and information**.

## SENATE REPORT - MAJORITY VIEW

The Report supported the rationale of the Bill and concluded that the Bill should be enacted subject to the following four recommendations, of which three relate to **regional media issues** which is a highly sensitive area within the Coalition of Liberal and National Parties comprising the Government:

- where a media company has a cross-media exemption, it be required to **disclose its relevant cross-media holding** when it reports on issues or matters relating to that holding (for example, when there is a cross-promotion);
- the Government consider extending its requirement for the provision of local news and information by regional media companies the subject of a cross-media exemption certificate to **all** regional media companies irrespective of cross-media interests provided that there is sufficient flexibility so as not to undermine the financial viability of regional broadcasters;
- in regional markets, cross-media exemptions should only be allowed in relation to proposals that could result in a media company having cross-ownership in **only two** of the three generic categories of newspapers, radio and television. This effectively maintains a cross-media restriction on a company controlling all three media operations in one licence area;
- the Government investigate the feasibility of providing appropriate **incentives** for regional media to provide local content, such as licence rebates.

## DISSENTING MINORITY VIEW

A minority dissenting report by the ALP and Australian Democrat members of the Committee opposed the rationale of the Bill in respect of cross-media ownership, arguing that the Bill would result in concentration of media ownership amongst three commercial media companies which is against the public interest. They rejected the Government's view that new technology such as the Internet has resulted in greater diversity in media because of the dominance of existing media companies in new platforms.

The dissenting report was highly critical of the exemption certificate regime on the basis that it was ineffective and overly interventionist. It also raised the issue that the regime may be open to legal challenge on the basis of it being unconstitutional in respect of its regulation of newspaper editorial processes.

The Australian Democrats opposed amendments media-specific foreign ownership restrictions that would allow foreign control of media operations. Conversely, the ALP was supportive in principle of the provisions in the Bill which allow foreign control provided that national interest considerations remain.

## CONCLUSION

The Government will most likely proceed with amending the Bill to address the concerns raised in the majority Report and introduce the Bill into Parliament. However, the substantial rejection of the Bill by the minority parties in the Senate is going to make it difficult for the Government to enact the Bill.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Raani Costelloe is a Senior Associate at the Sydney office of Allens Arthur Robinson***

# An Overview of New Zealand's New Telecommunications Regulatory Regime

**Seth Eeles examines New Zealand's new approach to telecommunications regulation.**

## OVERVIEW

Following the recommendations of the Ministerial Inquiry into Telecommunications, the New Zealand Government decided to establish a regulatory scheme specific to the telecommunications industry. This marked a shift away from New Zealand's previous reliance on general competition law for regulation of the industry.[1] While the scope of the new regulatory regime is carefully limited, its relative simplicity and specified decision timeframes may well produce more expeditious and efficient outcomes than more elaborate regulatory regimes.

The legislative basis for this scheme is the Telecommunications Act 2001 (**Act**). The Act has 5 primary components:

- The Telecommunications Commissioner;
- The Access System;
- The Telecommunications Service Obligations;
- General Network Regulation; and
- A System of Self Regulation.

## THE TELECOMMUNICATIONS COMMISSIONER

The Act establishes the new office of the Telecommunications Commissioner.[2] The Telecommunications Commissioner is a member of the Commerce Commission[3] who performs most of the new telecommunications-specific functions of the Commission under the Act. This new office and the additional functions of the Commission are funded by levy on industry participants.

## THE ACCESS SYSTEM

Part 2 of the Act sets up an access system based on the concept of Designated and Specified Services. These are the services regulated by the Act and are defined simply as those services described in Schedule 1 (see below for a list of initially Designated and Specified Services). In relation to Designated Services, the Commission has the power to determine both the price and non-price terms and the Act specifies initial and final pricing principles for each Designated Service. In relation to Specified Services, however, the Commission is restricted to determining the non-price terms of access. Schedule 1 of the Act provides a list of initial Designated and Specified Services along with various conditions and principles of access.

In addition, the Commission may make recommendations for the alteration of Schedule 1 which are in accordance with the purpose of this scheme which is stated to be:

> *"to promote competition in telecommunications markets for the long-term benefit of end-users of telecommunications services within New Zealand by regulating, and providing for the regulation of, the supply of certain telecommunications services between service providers."*[4]

The Act goes on to state that:

> *"In determining whether or not, or the extent to which, any act or omission will result, or will be likely to result, in competition in telecommunications markets for the long-term benefit of end-users of telecommunications services within New Zealand, the efficiencies that will result, or will be likely to result, from that act or omission must be considered."*[5]

Designated Services are further split up into Access Services and Multinetwork Services. A Multinetwork Service appears to be a service that involves more than 2 access providers such as number portability, whereas an Access Service appears to be a service provided bilaterally between an access provider and an access seeker (eg interconnection, retail services).

The list of initial Designated and Specified Services is set out below.

**Designated Access Services**

- Interconnection with Telecom's fixed PSTN;
- Interconnection with fixed PSTN other than Telecom's;
- Retail services offered by means of Telecom's fixed telecommunications network;
- Residential local access and calling service offered by means of Telecom's fixed telecommunications network;
- Bundle of retail services offered by means of Telecom's fixed telecommunications network; and
- Retail services offered by means of Telecom's fixed telecommunications network as part of bundle of retail services.

**Designated Multinetwork Services**

- Local telephone number portability service;
- Cellular telephone number portability service;
- National toll-free telephone number portability service; and
- Telecom's fixed PSTN to mobile carrier pre-selection service.

**Specified Services**

- National roaming;
- Co-location on cellular mobile transmission sites; and
- Co-location of equipment for fixed telecommunications services at sites used by Broadcast Communications Limited.

In addition to various conditions and principles for certain specific services, Schedule 1 also sets out the following standard access principles for each Designated Access Service and Specified Service:

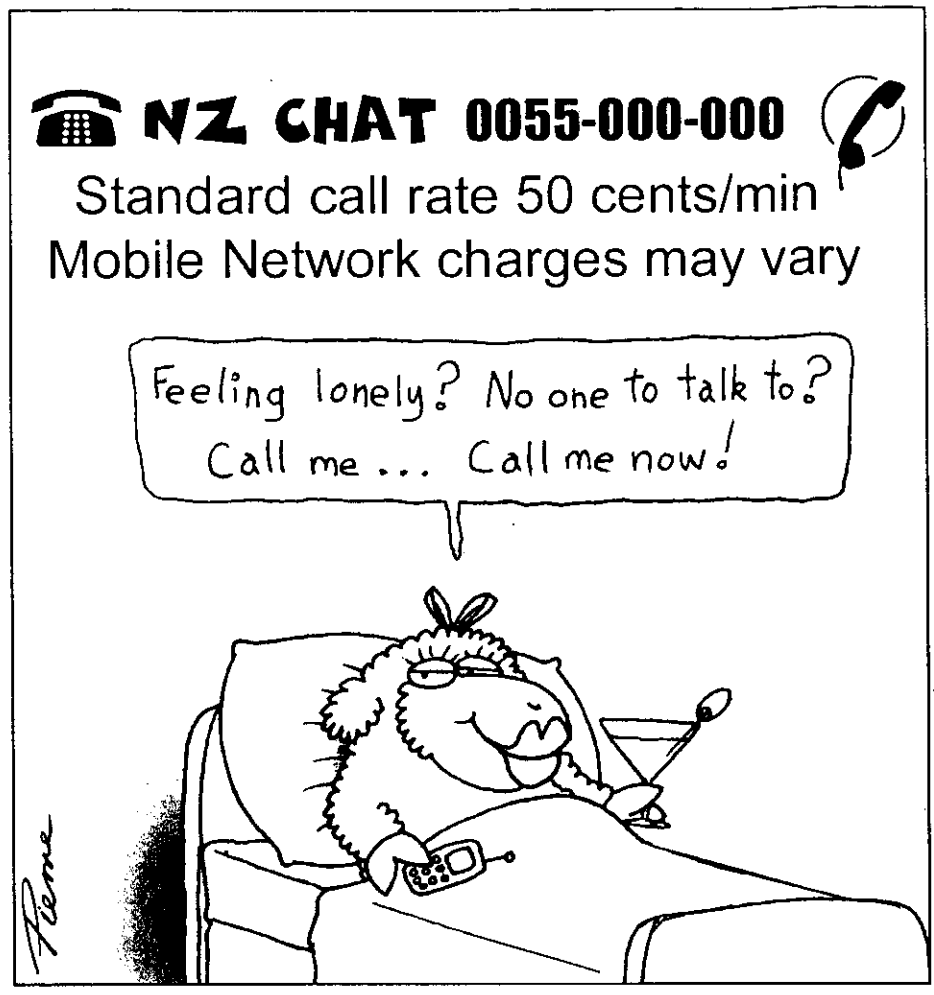
- the access provider must provide the service to the access seeker in a timely manner;
- the service must be supplied to a standard that is consistent with international best practice; and
- the access provider must provide the service on terms and conditions (excluding price) that are consistent with those terms and conditions on which the access provider provides the service to itself.[6]

These are in turn subject to the following limitations:

- reasonable technical and operational practicability having regard to the access provider's network;
- network security and safety;
- existing legal duties on the access provider to provide a defined level of service to users of the service;
- the inability, or likely inability, of the access seeker to comply with any reasonable conditions on which the service is supplied; and
- any request for a lesser standard of service from an access seeker.[7]

Although the government has emphasised the importance of commercial negotiations for the resolution of access disputes[8], the remainder of Part 2 of the Act provides for a determination process where these negotiations are not successful. There are separate determination processes for Designated Access Services/Specified Services, Multinetwork Services and the review of pricing determinations. The determination processes specify timeframes which the Commission must make "reasonable efforts" to comply with (for example, the Commission must make reasonable efforts to prepare a determination that includes the price payable for a Designated Service not later than 50 working days after giving notice of its decision to investigate[9]).

Since the commencement of the Act, the Commission has received applications for determinations from Telecom New Zealand in relation to interconnection services and TelstraClear and in relation to both interconnection and wholesale services. The Commission decided to investigate the interconnection service applications jointly and to limit the TelstraClear wholesale service application as it decided that TelstraClear had provided insufficient information to decide whether certain requested services fell within the definition of Designated Access Services. The Commission has also conducted consultations into the appropriate methodologies for the pricing of various designated services.




## THE TELECOMMUNICATIONS SERVICE OBLIGATIONS

Part 3 of the Act sets up a new and more flexible universal service scheme to supplement or replace the existing Kiwi Share Obligation (**KSO**)[10] called the Telecommunications Service Obligations (**TSO**). The KSO effectively required Telecom to provide a certain basic basket of services to residential customers at a fixed price (or at no per call charge, in the case of local calls) irrespective of the location of the customer or cost of providing the service to the customer. KSO losses were then recovered through the inteconnection fee.

The purpose of the TSO is to:

> *"facilitate the supply of certain telecommunications services to groups of end-users within New Zealand to whom those telecommunications services may not otherwise be supplied on a commercial basis or at a price that is considered by the Minister to be affordable to those groups of end-users"*[11]

The TSO in New Zealand is broader and more flexible than the "loss making service area" model adopted in Australia. The USO fund in Australia is calculated purely on a geographic basis and is therefore limited to rural and remote areas where sparseness of density increases the costs per customer to such an extent that the customer becomes loss making. In New Zealand, while geographic proximity is recognised as a contributing factor towards the affordability of telecommunications services, there are other issues which also do so.

Like Australia, the New Zealand TSO is not limited to Telecom (although see below for comments regarding the roll-forward of the Kiwi Share scheme). Any "service provider" is able to meet the TSO, as described further below.

Legislatively, the TSO is established by a TSO instrument. In accordance with section 70(4) of the Act, a TSO instrument must:

- record a contract or arrangement or an understanding between the Crown and a service provider for the supply of a particular telecommunications service or range of telecommunications services;
- identify the group of end-users to whom the service must be supplied;
- define the geographical area within which the service must be supplied;
- specify the retail price at, or below which, the service must be supplied; and
- specify the criteria that must be met for the standard of the service to be supplied.

Sections 70-71 provide for the Telecom KSO to become a deemed TSO Instrument and for its replacement with a "new KSO". In December 2001, the Government and Telecom entered into a deed that operates in place of and in addition to the KSO. Despite this, the TSO system allows for TSO Instruments with service providers other than Telecom and section 70(3) requires the Minister to assess whether each of the obligations of a TSO Instrument is contestable.

Subpart 2 of Part 2 provides for contributions for the cost of compliance with the TSO from other operators based on revenue. Subpart 3 allows the government to enforce a TSO Instrument via the courts.

Since the commencement of the Act, the Commission has conducted a consultation process to determine the implementation and costing of the TSO.

## GENERAL NETWORK REGULATION

Part 4 of the Act creates a system of voluntary registration as a network operator to "facilitate entry into, and competition in, telecommunications markets"[12]. Although telecommunications service providers need not apply for network operator status, such a declaration provides certain powers with respect to the entry of land and the construction/maintenance of a network. Part 4 also makes rules relating to networks generally including rules for connection to and the misuse of a network.

## SELF REGULATION

Schedule 2 of the Act allows for the preparation of telecommunications access codes by an industry forum in relation to Designated and Specified Services and for the process of variation and/or approval of such codes by the Commission.

Telecommunications access codes can only provide for:

- procedures, requirements, and other matters, not inconsistent with the Act, in respect of the implementation of applicable access principles with respect to Designated Access Services or Specified Services; or
- the functions that must be performed by a system for determining the service and the standard to which those functions must be performed with respect to a Designated Multinetwork Service.[13]

Such codes cannot provide for the implementation of pricing principles in relation to designated access services or the apportionment of the cost of delivering a Multinetwork Service.

Although there appears to be nothing preventing the forum from creating codes relating to services that are not designated or specified, such codes would not be covered by the operation of the Act.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Seth Eeles is a lawyer with Gilbert and Tobin, Sydney***

1 For a discussion of this shift, see "Beginning of the End of "Light Handed" Telecommunications Regulation in New Zealand" by Tristan Gilbertson (http://203.111.11.66/templates/publications/default.jsp?pubid=296)

2 See part 1 of the Act

3 The Commerce Commission is New Zealand's equivalent of the ACCC.

4 Section 18(1)

5 Section 18(2)

6 Schedule 1, Subpart 2, clause 5

7 Schedule 1, Subpart 2, clause 6

8 An indication of this is the requirement that any party applying for a determination for a designated access service must demonstrate that they have "made reasonable attempts to negotiate the terms of supply of the service".

9 Section 28(1)(b)

10 This was Telecom's existing universal service obligation.

11 Section 70(1)

12 Section 102(1)

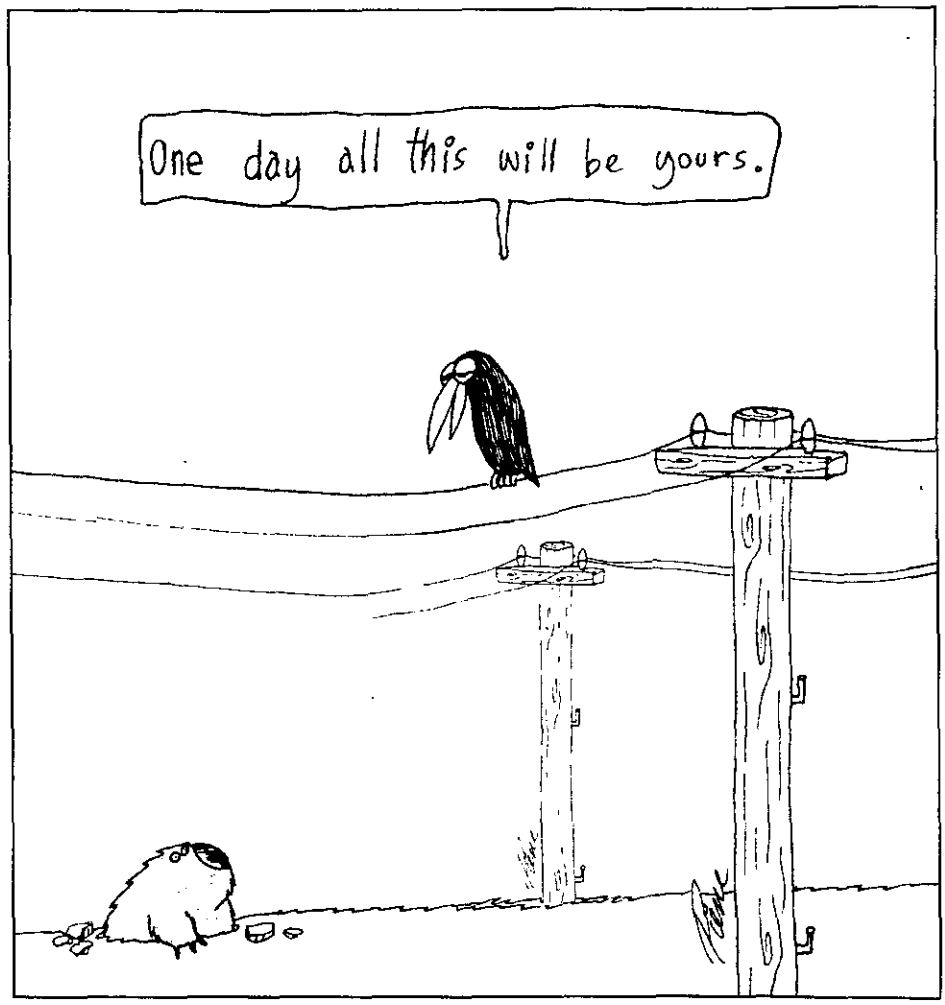
13 Schedule 2, clauses 2 & 3

# Telstra Corporation Ltd. v Hurstville City Council, Optus Vision Pty Limited v Warringah Council - The Decision of the Full Federal Court

**Angela Brewer updates the progress of this watershed case regarding telecommunications infrastructure.**

Earlier this year the Full Federal Court delivered its decision in *Telstra Corporation Ltd. v Hurstville City Council; Optus Vision Pty Limited v Warringah Council* [2002] FCA 385 (4 April 2002). This judgment reversed the earlier decision of Justice Wilcox who had found that telecommunications carriers were subject to local government charges under section 611 of the *Local Government Act* 1993 with respect to the telecommunications infrastructure they had installed over and under public land. This judgment was seen as a great success for the Councils in upholding the charges and rates in respect of cables by Councils throughout NSW and Victoria.

The Full Federal Court, reduced to a bench of two judges due to illness and comprising Justices Sundberg and Finkelstein, found in favour of the carriers on only one ground of appeal relating to clause 44 of Schedule 3 of the *Telecommunications Act* 1997 ("**Act**"). The Court declined to determine the question of whether charges under section 611 were an excise, contrary to section 90 of the Constitution. In relation to the question of whether the charges were levied by the councils for an improper or extraneous purpose, the Full Federal Court stated that they agreed with Wilcox J, finding "that the purposes alleged to be extraneous" were not in fact extraneous.




## WHETHER SECTION 611 CHARGES ARE DISCRIMINATORY

At first instance, Justice Wilcox left undecided the question of whether the application of charges under section 611 were discriminatory against carriers having regard to clause 44(1) of Schedule 3 of the Act. On appeal, the Court found in favour of the carriers on this ground.

The Court held that section 611, to the extent that it authorised councils to levy and recover charges in respect of cables erected or placed on, under or over a public place, was discriminatory and therefore invalid pursuant to clause 109 of the Constitution.

The Court relied upon a dissenting judgment of Justice Stevens in a United States Supreme Court decision of *Department of Revenue of Oregon v ACF Industries* 510 U.S. 332 (1994) to support its finding. No further authority was cited in support of the Court's decision.

With the Full Federal Court declining to determine the issue of excise and supporting the finding of Wilcox J in relation to extraneous purpose, the

judgment in favour of Telstra and Optus may not give the carriers the level of comfort they require.

## HIGH COURT CHALLENGE - COUNCILS TRIUMPHANT?

The decision of the Full Federal Court did not represent a resounding win for telecommunications carriers. Of the four grounds of appeal raised, the Full Federal Court only determined two issues:

- discrimination, which they based upon the judgment of a single dissenting judge of the United States Supreme Court; and
- extraneous purpose, they formed the view that the purposes alleged to be extraneous were not.

The Councils of NSW and Victoria have filed Applications for Special Leave with the High Court seeking orders that the judgment of the Full Federal Court be set aside on the grounds that the Full Federal Court erred in finding that section 611 discriminates against telecommunications carriers. Additionally, the Councils now seek an order that the Full Federal Court erred in its finding that it was not appropriate to deal with the question of whether section 611 imposed a duty of excise.

With the Application filed, we must now wait to see whether the High Court will grant the Councils leave to challenge the findings of the Full Federal Court. It is anticipated that the special leave application will be heard by the High Court later this year.

The grant of special leave to appeal by the High Court is discretionary. For special leave to be granted, the matter has to be one of either public importance or interests of justice require that leave be granted. Arguably, this case is one such matter of public importance as it involves the question of construction of section 51(v) of the Commonwealth Constitution. The characterisation which has been placed upon that section by the Full Federal Court is one which would significantly broaden Commonwealth power. This case also raises important questions concerning the interrelationship between Commonwealth and State laws, including the manner in which section 109 of the Constitution operates; and the use of public lands of New South Wales and Victoria, and potentially all other States of Australia.

This is a matter with significant implications for Commonwealth – State relations in Australia. As such it is a matter in which in the writer's view, it would be appropriate for the High Court to grant special leave to the Councils of New South Wales and Victoria.

## PUSH TO PLACE CABLES UNDERGROUND

Outside the court room telecommunications cables have again come under the spotlight.

There is current report before the State Government which proposes that all of Sydney's electricity cables be placed underground. The report acknowledges that such a move would costs as much as $5000 a household and discusses alternative methods of funding the push underground. The report has received wide community and government support.

Local Government has been a continuing advocate of putting cables underground. Councils' stance found its way into the present action where, at first instance, Telstra and Optus sought to argue that the decision of the NSW Councils to make and levy a charge on telecommunications carriers in respect of cables was taken for a purpose extraneous to section 611 of the Local Government Act – namely to penalise the installation of above-ground telecommunications cables and to discourage further installation of any such cables. Evidence showed that many councils levied a higher rate or charge for cables which were above ground compared to the rate charged for cables which were below ground. Although there was a disparity between the charges, Justice Wilcox found against the telecommunications carriers' assertion.

With such a strong push by the State Government to put electricity cables underground, telecommunications carriers must be looking at the road ahead and asking how long it will be before they too must place their cables underground.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Angela Brewer is Solicitor at the Sydney office of Deacons.***

# Interception Law Under Scrutiny

**On the anniversary of September 11, Ben Kuffer reviews the rise and fall of a key plank in the government's post September 11 2001 reforms.**

## INTRODUCTION

The Federal Government's widely criticised hardline response to the September 11 2001 terrorist attacks has been dealt a blow, with the Senate rejecting certain controversial proposed amendments to the *Telecommunications (Interception) Act 1979* ("**TIA**"). The impact of the aboutface means, at least for now, a victory for privacy in the telecommunications sector and a continuing level of confusion for certain telecommunications sector participants such as internet service providers.

This article reviews the key components of the TIA and the proposed amendments, considers whether the TIA remains effective in light of dramatic changes in technology and policy since its inception, and considers whether Australian's have missed yet another opportunity for debate. The article does not consider the more specific procedural amendments proposed by the Bill such as the proposed amendments to the TIA relating to the Western Australian Anti-Corruption Commission, the Royal Commission into Police Corruption or the NSW Independent Commission Against Corruption[1].

## HISTORY OF THE *TELECOMMUNICATIONS (INTERCEPTION) ACT 1979*

The TIA details the rights and responsibilities of Australian's in relation to the interception of communications. On its introduction, the TIA significantly expanded the grounds for which telephone interception may be authorised. Due to the increasing use of computers and electronic technology, the TIA extended the scope of protection from interception to include other telecommunications services such as data transfer systems[2].

The TIA is a tool used to regulate the access of law enforcement agencies to private communications. The TIA became the secure legal basis for the use of telephone intercepts for general law enforcement purposes[3] but this was coupled with an "objective to protect the privacy of telecommunications passing between users of telecommunications systems"[4]. The tension in the TIA is that it is per se an offence to intercept telecommunications but this is balanced with Parliament's and the broader community's law enforcement and national security interests.

Commentators have noted that "in Australia the legislation governing the interception of communications is not entirely satisfactory"[5] and the TIA has been described as "a model of legislative obscurity, being confusing, circular and verbose"[6].

## CASE LAW - WORKINGS OF THE TIA

It is useful to drill-down into the workings of the TIA and, by reference to case law, to determine exactly what is permitted and prohibited in relation to intercepting communications in the Australian telecommunications system.

Interception is defined in section 6(1) of the TIA as:

> *"...interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such communication in its passage over that telecommunications system without the knowledge of the person making the communication".*

### (a) Telecommunications System

The TIA only applies to communication passing over a "telecommunications system", and as such the definition of telecommunications system is critical. The definition of "telecommunications system" and "telecommunications network" contained in section 5 of the TIA have the effect of limiting the application of the TIA to communications which pass over a system or series of systems for carrying communications by means of guided or unguided electromagnetic energy or both, and includes equipment, a line or other facility that is within Australia, but does not include a system or series of systems for carrying communications solely by means of radiocommunications[7]. If a communication is made solely by means of radiocommunication it may be intercepted without infringing the TIA.

The distinction between radio communications (a form of unguided electromagnetic energy) and the definition of "telecommunications network" contained at section 5 of the TIA is unclear. However, the TIA has been amended so that the definition of telecommunications system now more clearly includes mobile telephony.

The current definition of telecommunications system is broad enough to cover technological advancements that we know about at present, such as optic fibre and other opto-electronic developments, because these new developments are guided or unguided[8]. The problem, however, is whether there is sufficient flexibility in the legislation to cover what has not yet been invented and to distinguish any 'new' telecommunications network (as defined) from a radiocommunications network.

### (b) Passing Over

As described above, another component of interception under the TIA is the fact that the communication must be "passing over" the telecommunications system. Numerous cases have considered what is meant by the term passing over and the Courts have applied a technical test to determine same[9]. The Criminal Court of Appeal in *Edelsten* upheld Lee J.'s decision in the original *Edelsten* trial[10] to reject an argument put forward by the plaintiff that electromagnetic waves picked up by a scanner were free in the air and not passing over a telecommunications system. The judge held that the mobile phone's electromagnetic waves were in fact part of a system controlled by the then Telecom which had control of the transmitting and receiving unit. The means used to listen to or record the signal in the course of the passage over the telecommunications system was held by the court to be irrelevant[11].

Passage over a telecommunications system was also considered by the judiciary in *Miller v Miller (1978)*[12] ("***Miller***"). Here the High Court applied an earlier 1960 Act and, among other things, concluded that the 1960 Act was inconsistent with the State listening devices legislation[13] and to the extent of the inconsistency, the 1960 Act applied. In essence the High Court, by accepting that the Commonwealth Act applies, concluded that the recording of a

conversation by a party lawfully on a premises but eavesdropping on another extension did not constitute interception of a communication passing over a telecommunications system and was therefore admissible in the original Family Court proceedings because the listener was lawfully on the premises and the communication at a second extension was passing over the telecommunications system. The judgment in *Miller* allowing the admission of the recorded phone call between the mother and child at the centre of a custody dispute goes against Sackville J.'s comments in *Taciak* which suggest a "restrictive approach to the construction of the statutory exceptions to the prohibitions on the interception of telecommunications and on the use of lawfully obtained intercept information"[14].

In *Harvey v Baumgart (1965)*[15], Gowans J held that "passing over" required an element of "automatic simultaneousness"[16]. In *R v Curran*[17] McGarvie J held that a portable tape recorder held to the earpiece of a telephone which was being used by another person illegally (ie a wire had been run so that a legitimate service was being charged for another person's calls) was not an interception because the recording of the communication passing over the telecommunications system was done by equipment not part of the service[18]. See further *R v Luciano Giaccio* SASC 6103 (1997)[19].

McGarvie J distinguished the decision of Cosgrove J in *R v Migliorini*[20] because the tape recorder in that instance was attached directly to the wire and made its recording "directly by the electromagnetic energy passing through the service"[21]. Cosgrove noted that the legislation would not capture an external recording device but McGarvie disagreed with this limited construction[22] of interception and, following the decision in *Miller* held that an external tape recorder held up to an earpiece recording the sounds being emitted was in fact recording of a communication passing over the telecommunications system. This interpretation was confirmed by the minority in *T v The Medical Board of South Australia (1992)*[23] (***"T v Medical Board SA"***) and the decision in *Miller* by the majority is inconsistent with *T v Medical Board SA*.

**(c) Without the Knowledge**

The third element of the definition of interception of a communication is that the interception must be made "without the knowledge" of the person making the communication. In *T v Medical Board SA*[24] interception was held to occur if a third party intrusion into a communication was made without the knowledge of the caller or the recipient[25]. The TIA offers no protection as between the caller and the intended recipient, but only against an invading third party[26].

## PROHIBITION ON INTERCEPTION – SECTION 7 OF THE TIA

Section 7(1) of the TIA prohibits the interception (as defined above) of communications passing over the telecommunications system in the following circumstances;

> *"A person shall not:*
>
> *(a) intercept;*
>
> *(b) authorize, suffer or permit another person to intercept; or*
>
> *(c) do any act or thing that will enable him or her or another person to intercept;*
>
> *a communication passing over a telecommunications system"*

## EXCEPTIONS TO THE PROHIBITION

These prohibitions are subject to certain exceptions which allow for interceptions to be made in connection with certain activities including, without limitation, interception of a communication by a person;

- who is an employee of a carrier in the course of his or her duties for or in connection with, among other things the installation of any line or equipment used or intended for use in connection with a telecommunications service[27], the operation or maintenance of a telecommunications system[28] or the identifying or tracing of any person who has, is suspected of or is likely to contravene a provision of Part VIIB of the *Crimes Act 1914*[29] where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively;
- who is another person lawfully engaged in duties relating to the installation or maintenance of equipment or a line[30];
- who is lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for the interception of communication under warrants[31];
- which is incidental to, or results from action taken by an officer of the Australian Security Intelligence Organisation in discovering where a listening device is being used at or is located[32];
- under a warrant[33]; or
- in an emergency (as defined in section 30 of the TIA)[34].

It is important to note that the stipulation that communications may not be intercepted is also waived (i.e. in addition to those exemptions listed above) if an officer of an agency[35] is a party to the conversation and there are reasonable grounds for suspecting that another party to the communication has, among other things, caused or threatened to cause serious injury, killed or threatened to kill another person, seriously damaged property or threatened to take his own life. The provisions of s. 7(6) of the TIA give broad powers to certain officers to retrospectively apply for Class One and Class Two warrants in an 'emergency' situation.

## TELECOMMUNICATION INTERCEPTION WARRANTS

The issuing of interception warrants by the Attorney-General to ASIO and other law enforcement agencies is subject to specific and detailed regulations. In the case of law enforcement agencies, warrants may be issued to assist in the investigation of certain serious offences as defined in sections 5 and 5D of the TIA[36]. Warrants can be obtained in relation to particular identified telecommunications services or any telecommunication service that is used or is likely to be used by a named individual.

## WHAT IF THE TIA DOES NOT APPLY?

The above cases and the development of judicial opinion has shown that as a general rule listening in to or recording communications using equipment which is "electronically connected into or which intercepts radio signals transmitted by a telecommunications system"[37] is covered by the TIA. If the equipment is external to the telecommunications system then the State based listening devices legislation applies[38]. This is reinforced by Barwick

CJ in *Miller* who states, "the TIA does evince a clear intention to be the whole law on the matter of telephonic interception"[39] and, as a result, holds that the TIA prevails over the State based legislation. This is consistent with the provisions of s. 109 of the *Constitution*[40]. If the State based legislation does not apply then the standard search warrant provisions apply.

Telecommunications interception is also dealt with under the *Telecommunications Act 1997* (**"TA"**). This article does not attempt to deal with the provisions of the TA, suffice to note that the essential difference between the TIA and the TA in respect of telecommunications interception is that the TIA "makes it an offence for anyone, subject to certain exemptions to intercept telecommunications"[41] whereas Part 13 of the TA makes it an offence for people in the business of telecommunications to disclose or use confidential communications that come into their knowledge or possession through their legitimate business.

## TELECOMMUNICATIONS INTERCEPTION LEGISLATION AMENDMENT BILL

On 27 September 2001, the *Telecommunications Interception Legislation Amendment Bill (2001)* (**"2001 Bill"**) was introduced before the House of Representatives. The 2001 Bill had not passed either Chamber before the Parliament was prorogued for the 2001 Federal Election and consequently it lapsed.

On 12 March 2002, after the federal election had been held and importantly the world had experienced the dramatic events of September 11 2001, the now amended *Telecommunications Interception Legislation Amendment Bill (2002)* (**"2002 Bill"**) was re-introduced into the House of Representatives by the Attorney General. The 2002 Bill expanded on the 2001 Bill by including a new offence (act of terrorism) for which a telecommunications interception warrant may be sought. The 2002 Bill was introduced by the Federal Government as one component of a suite of some five anti-terrorism bills[42]. Amid a storm of controversy the 2002 Bill was passed the next day by the House of Representatives and introduced into the Senate on 14 March 2002.

The Senate refused to pass the suite of bills and demanded an enquiry be conducted by the Senate Legal and Constitutional


Legislation Committee (**"SLCLC"**). This report has been tabled and contains significant recommended amendments to the 2002 Bill and the other 5 anti-terrorism bills. There has been an outcry, indicated by the a total of 431 submissions to the SLCLC, in relation to the legislation and the unwillingness of bi-partisan members of the Senate to rush to pass the bills notwithstanding the panic that followed 11 September 2001. The Committee's report (**"SLCLC Report"**) was released in early May 2002 and it contained some key recommendations in relation to both suite of anti-terrorism bills and specifically the 2002 Bill[43].

Although some amendments to the TIA did carry, the Senate rejected amendments that would have allowed law enforcement agencies to access, without a warrant, the content of messages such as email, voicemail and SMS, while such communications were delayed or temporarily stored on a telecommunications service providers' equipment during transit.

The purpose of the 2002 Bill was to amend the TIA[44] to, among other things;

- expand Class 1 and Class 2 offences to include offences constituted by conduct involving acts of terrorism, child pornography and serious arson[45]; and
- legislatively clarify the application of the TIA to telecommunications services involving a delay between the initiation of the communication and its access by the recipient, such as email and short messaging services[46].

### (a) New Offences

As stated above, the 2002 Bill expanded the Class 1 and Class 2 offences in relation to which a telecommunications interception warrant may be sought.

The Federal Attorney-General, in the Second Reading Speech for the 2002 Bill stated, in relation to the proposed amendments dealing with "terrorism" as an offence, that "these provisions and other measures taken" (that is the suite of bills introduced as part of the terrorism legislation), "are designed to bolster our armoury in the war against terrorism and deliver on our commitment to enhance our ability to meet the challenges of the new terrorist environment"[47].

The proposed amendments do not define what is meant by an offence being that

'constituted by conduct involving an act or acts of terrorism'. The Explanatory Memorandum to the 2002 Bill states that the reason for this is so that intercepting agencies are able to seek interception warrants in connection with terrorism offences howsoever they are defined in relevant legislation[48]. It is unclear as to what these offences are. This is a significant risk to the privacy of users of the telecommunications system.

The Senate passed the proposed new Class 1 and Class 2 offences, with the exception of 'terrorism'. However, the Government stated that it intended to reintroduce this provision in the spring sitting of parliament. If terrorism is included as a Class 1 offence it will be less well defined than the other Class 1 offences of the TIA. Also, due to its classification as a Class 1 offence it will be subject to significantly less preconditions for the issuance of a warrant than the stringent conditions used to determine the result of an application for a Class 2 warrant[49]. This amendment is clearly a reaction to 11 September. The underlying theme of the SLCLC Report and submissions relating to it suggests that the amendments have been rushed and ill-planned.

**(b) Delayed Access Message Services**

The other controversial amendment to the TIA is the proposed new sections 6(3)-(5) which deal unsatisfactorily with the concept of delayed access message service[50]. Of the 400 plus submissions to the SLCLC, only a select few mentioned these amendments which attempt to indicate when delayed access message services, such as emails and voicemail, will be regarded as communications passing over a telecommunications system and thus subject to the TIA and the requirements surrounding interception warrants.

These provisions were also rejected by the Senate. As with the terrorism provision, the Government has also stated its intention to reintroduce the delayed access message service amendments into parliament later in the year. For this reason, analysis of these proposed amendments is relevant.

The Attorney-General in his second reading speech stated:

> *"The amendments make it clear that a communication will fall outside the definition of interception where it is stored on equipment and can be accessed using that equipment but without reference to the telecommunications network"*

In that event, agencies will be able to access the communication using a search warrant or other means with a less stringent test for issuance. It is not clear if, as indicated in submissions, the 2002 Bill intended to protect emails from the time they are sent to the point at which they have been downloaded to a recipient's computer[51]. They in fact may not be protected for anywhere near as long as that indicated under the amendments depending on the technology used by the recipients email provider and his method of accessing same[52].

Problems also arise with messages stored on an ISP's server as such messages can be accessed by the equipment on which it is stored without using a telecommunications line. Access to these communications is available to anyone with access to the ISP's premises and computer passwords. The key risk is that an agency possessing only a search warrant, or merely a certificate issued under Part 13 of the TA, may access such communications in this way rather than acquiring an interception warrant[53].

The relevant section of the 2002 Bill sought to insert at the end of the TIA section 6, (from above the clause dealing with what constitutes an interception for the purposes of the TIA), certain provisions which indicate when delayed access message services such as email and voicemails will be regarded as passing over a telecommunications system and thus subject to the protection of the TIA.

The essential problem with the proposed amendments is the arbitrary distinction drawn in relation to the form of access. If, for example, a person needs to access a telecommunications service in order to access an email or voicemail message then an interception warrant is required. If however, the same voicemail or email can be accessed from a company's premises without the use of the telecommunications system, for example potentially if the voicemail is digitised and stored on a computer hard-drive or an email is stored on a server, then the provisions of the TIA will not apply[54]. In that event some other lawful authority will be required before a third party could access the message or email[55]. The probable reason for this is that, if a message isn't passing over a communications system, it may be beyond the scope of section 51 of the Australian Constitution.

The proposed amendments may lead to the situation where voicemail and email at the service provider's location are not protected by the TIA and may be accessed with a search warrant, however a telecommunications interception warrant will be required at the time that the intended recipient accesses the messages.

The proposed definition of delayed access message service is also problematic in relation to the GSM mobile phone short message service ("SMS"). Under the proposed amendments an SMS message in its passage to a handset would be protected by the TIA but once it is opened or stored on the phone's SIM card it would no longer be covered by the TIA. Likewise, as with an email message, once it has been downloaded or replicated to a computer hard drive whether or not at the point of downloading the message has been opened.

## IMPACT OF PROPOSED AMENDMENTS

The focus of Australia's telecommunications regulatory framework is that of a light touch self-regulation based model with significant consumer protections[56]. A key aspect of the consumer protection provisions is for codes of conduct to be developed consultatively by all stakeholders in the industry. The Australian Communications Industry Forum (**"ACIF"**), an industry body established to manage the telecommunications industry's response to self-regulation through a system of committees and working groups made up of representatives from the industry, consumer groups and the various regulators, has facilitated the development of a voluntary guidelines entitled "Participant Monitoring of Communications"[57]. The guidelines are intended to provide guidance to call centres, carriage service providers and carriers who have need to monitor communications by other people within the relevant organisation (eg supervisor).

The ACIF guideline is a valuable resource for participants in the telecommunications industry and provides a good summary of the Act from a practical perspective. The guideline must be updated to include the significant recent amendments when and if they are passed through parliament. There may be particular difficulty for ACIF in interpreting the amendments. To be relevant to an ISP for example, any new ACIF code or guideline would need to clarify whether an agency is entitled, without an interception warrant, to access communications stored on an ISP's server[58].

Currently, some ISP's are refusing access to data without a telecommunications interception warrant[59]. The proposed amendments, as currently drafted, may permit the agencies to access the communication without an interception warrant.

In its submission to the Senate Enquiry, the Office of the Federal Privacy Commissioner questioned why the 2002 Bill sought to remove the privacy protection via the requirement of an interception warrant in relation to a voicemail or SMS merely because they transmission is delayed[60]. With the December 2001 amendments to the Commonwealth *Privacy Act*, and a heightened public and political awareness of the issue, it remains to be seen whether the government will risk removing an important privacy protection mechanism from the playing field.

## CONCLUSION

The rejection of the proposed amendments is an initial victory for common sense and privacy in Australia. However, it remains to be seen if the legislative clarification required to establish a logical and consistent system of intereception, which is able to deal with new technology such as SMS, actually eventuates.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Ben Kuffer is an Associate in the Information, Communications and Technology Group at PricewaterhouseCooopers Legal, Sydney.***

1 Other amendments proposed include, without limitation, those relating to the removal of references to defunct State bodies and the substitution of replacements.

2 See TIA at s.5 "Communication" which is defined to mean "conversation and a message... in the form of *(among other things)* speech, data, text and visual images". The definition of "Telecommunications Network" is also instructive in that it is so broad as to include both guided and unguided electromagnetic energy.

3 *"Electronic surveillance, human rights and criminal justice"*, Simon Bronitt, Australian Journal of Human Rights, 3(2), 1997, at p.188, as referred to in Dept of Parliamentary Library

4 *Alan Taciak v Commissioner of Australian Federal Police ("**Taciak**") (1995)* NG 476, Unreported, at 24.

5 *"Controlling the Interception of Communications: Law or Technology?"*, RG Smith, Australian Institute of Criminology, 1997, at p.1.

6 *"Aspects of Criminal Investigation: Arrest, Search and Seizure, Listening Devices and Telephone Taps"*, D.Re, paper presented at Young Lawyers, Continuing Legal Education Seminar, 16 August 1995, as cited in Smith.

7 s.5 TIA, see further *"Controlling the Interception of Communications: Law or Technology?"*, RG Smith, Australian Institute of Criminology, 1997, at p.3.

8 *Personal conversation with D.J.Bowman*, UNSW Physics and Bio-medical Engineering.

9 *"Participant Monitoring of Communications"*, Australian Communications Industry Forum G:516, July 1998 at 4.3.

10 *R v Edelsten* (1990) 21 NSWLR 542 at 548.

11 Ibid at 549.

12 *Miller v Miller (1978)* 141 CLR 269.

13 Barwick CJ in *Miller* states that, "The 1960 Act *(sic)*does evince a clear intention to be the whole law on the matter of telephonic interception: nor should such a conclusion be surprising for the telephone system is provided and administered by an Australian instrumentality under Australian law".

14 Op cit note 4 at 27.

15 *Harvey v Baumgart (1965)* 7 FLR 389.

16 ibid at 393 and 395.

17 *R v Curran* (1982) 50 ALR 745 per McGarvie J.

18 Note that passing over was accepted by the Court and as it was an interception not permitted by the TIA, the court used its discretion to admit the recording on public interest grounds.

19 In this case Cox J states that In my opinion the taping of these telephone conversations by means of a micro-cassette recorder, held close to the telephone hand-piece by one of the persons having the conversation, did not amount to an interception of a communication passing over a telecommunications system within the meaning of sections 6 and 7 of the Interception Act

20 *R v Migliorini (1982)* 38 ALR 356.

21 Ibid at 360.

22 *R v Curran* (1982) 50 ALR 745 at 767

23 See further Olsson J's judgment in *T v The Medical Board of South Australia* (1992), 58 SASR 382

24 Ibid per Matheson J at 397.

25 This decision was followed in *Carbone and Another v National Crime Authority and Others (1994).*

26 *Green v R* (1995) 135 ALR 81.

27 TIA, s. 7(2)(a)(i)

28 TIA s. 7(2)(a)(ii)

29 TIA s. 7(2)(a)(iii)

30 TIA s. 7(2)(aa)

31 TIA s. 7(2)(ab)

32 TIA s. 7(2)(ac)

33 TIA s. 7(2)(b)

34 TIA s. 7(2)(c)

35 Agency for the purposes of this part of the TIA means the Australian Federal Police, ASIO and eligible State agencies as declared by the Minister pursuant to s. 34 of the TIA. These agencies must also be listed in the corresponding year's Annual Report.

36 Op cit note 5, at p. 4.

37 *"Participant Monitoring of Communications"*, ACIF G516:1998, July 1998, at 4.4.

38 Op cit note 12

39 Op cit note 12 per Barwick CJ at 13.

40 The relevant constitutional law is not the topic of this paper other than to note that s.109 of the Constitution states that to the extent of any inconsistency between Commonwealth (i.e. TIA) and State (i.e. Listening Devices Act) laws, Commonwealth legislation shall apply. In *Miller*, Barwick CJ held that the was an inconsistency between the legislation brought about by a "manifestation of intention" by the Commonwealth Act that it be the whole with respect to telecommunications interception (Op cit note 12 per Barwick CJ at 12).

41 *"Australian Telecommunications Regulation"*, edited by Jock Given and Alasdair Grant, 2nd edition 2001, at p.229.

42 The five bills are; *Security Legislation Amendment (Terrorism) Bill 2002, Suppression of the Financing of Terrorism Bill 2002, Criminal Code Amendment (Suppression of Terrorist Bombing) Bill 2002, Border Security Legislation Amendment Bill 2002* and the 2002 Bill.

43 SLCLC Report, May 2002.

44 *"Telecommunications Interception Legislation Amendment Bill 2002"*, Department of Parliamentary Library Information and Research Service, Bills Digest No. 121 2001-2002 at p. 6..

45 *"Explanatory Memorandum - Telecommunications Interception Legislation Amendment Bill 2002"*, circulated by the Attorney-General, the Honourable Daryl Williams, at p. 2. As interception warrants can only be issued for Class 1 and Class 2 offences new offences are proposed in these classes to include terrorism, arson and child pornography.

46 ibid

47 *Hansard*, House of Representatives, 12 March 2002, p 977.

48 Op cit note 44 at p. 14.

49 Compare TIA s. 45 (e) re. Class 1 offence with 46(2) Class 2 offence.

50 This amendment only appeared in the 2002 Bill and not in the TIA amendments as originally tabled in the *Telecommunications Interception Legislation Amendment Bill 2001*.

51 Electronic Frontiers Australia, submission to the Senate and Constitutional Legislation Committee, 5 April 2002, Submission Number 134, at p 4.

52 An example may be the situation where an email is sent to a recipient who downloads the email by way of replication onto his hard drive and does not look at the email until some time later. The email would no longer be protected once off line unless the recipient logs in remotely to a server and downloads this mail over the telecommunications system.

53 Oz Net Law submission to the Senate Legal and Constitutional Committee

54 These are but some eventualities. It is highly probable that the interception provisions will only cover a small portion of delayed access message situations.

55 Explanatory Memorandum to the 2002 Bill, at p. 4.

56 *"Telecommunications and new technologies"*, Office of the Privacy Commissioner, www.privacy.gov.au, at p. 34.

57 Op cit note 33.

58 From above this is relevant because emails stored on the ISP's server are stored communications as they can be accessed by the equipment on which they are stored without using a telecommunications line.

59 *Hansard*, Legal and Constitutional Committee, 19 April 2002, p. 211.

60 Federal Privacy Commissioner Submission to the Senate Legal and Constitutional Legislation Committee, 15 April 2002, at p. 14.

# Invasive Technology & Privacy Implications

**Rebecca Sharman discusses the boundary of recent amendments to privacy laws when applied to new technologies.**

The Privacy Act 1988 (Cth) ("**Act**") regulates the collection and use of personal information. This is defined to include any information about an individual whose identity is apparent, or can reasonably be ascertained from the information. This article examines the concept of the "location" of a mobile phone user as personal information, the technology available for tracking mobile phone users and the benefits and risks involved with the use of this technology.

## "LOCATION" AS PERSONAL INFORMATION?

Due to recent technological developments it is now possible to track the location of mobile phone users with reasonable accuracy. It is arguable that the location of a mobile phone user (whether past or present), when coupled with their name, falls within the definition of 'personal information' in the Act. Even if an organisation simply records and stores 'location' data without identifying the individual, it may still be possible for someone with the aid of other material, to identify the individual.

Given that under the Act personal information need not need to be in a material form or accurate or even correct, a rough calculation of a persons' whereabouts may amount to personal information.

If the concept of "location" as personal information is accepted, then organisations collecting and/or using this information will be subject to the requirements of the Act and either the National Privacy Principles ("**NPPs**") or the Information Privacy Principles ("**IPPs**"). This will be discussed further below.

## TRACKING TECHNOLOGY

There are four types of tracking technology used to determine the location of a mobile phone telephone user. Firstly, the location of a mobile phone user may be determined by analysing the geographical position of the base station with which the mobile phone at that particular point of time is communicating. This method is universally available, however as it is dependant on the calculation of the distance between base stations; its accuracy ranging from 300m – 5km.

The second method is commonly known as 'triangulation'. At any one time, mobile phones send a signal, containing the phone's unique digital identity number known as "IMSI", to the surrounding network antennas. By comparing the strength of the signals and the time of arrival, mobile phone companies can triangulate the position of the user. These signals are sent regardless of whether the phone is switched on or whether the user is making or receiving a call. Using software, it is possible to generate the triangulation calculation automatically.

A more accurate method involves embedding a Global Positioning System (GPS) receiver into the mobile phone. The GPS receiver transmits location information to orbiting satellites. The GPS calculation enables the tracker to pin point the mobile phone user to within 10 metres.

The newest tracking technology is 3G broadwidth technology. It is alleged that this technology will enable mobile phone users to be tracked to the nearest metre.

## WHO USES TRACKING TECHNOLOGY?

It is now the case that if you carry a mobile phone you can be tracked. Knowing this, the next question to ask is, who is analysing this data?

### (a) Mobile Phone Companies

It is well known that mobile phone companies record, in real time, the signals transmitted by mobile phones to base stations. However, it is not known whether mobile phone companies link these signals in real time with the owner of the mobile phone. Mobile phone companies do make this link at a later stage for the purposes of billing.

While it may be necessary for mobile phone networks to know your location in order to communicate with your phone, the concern is that this information may be used for other purposes, or that someone may obtain unauthorised access to this information.

### (b) Government

In June Senator Natasha Stott Despoja, then leader of the Australian Democrats raised concerns about the powers of the Government to access phone records under the *Telecommunications Interception Act*. There is a loophole in the Act that enables authorities to access phone records held by mobile phone companies, in particular the location of callers, without a warrant. In the past 12 months it is estimated that 750,000 disclosures of phone details were obtained by officials without a warrant. Stott Despoja states "no warrants, no privacy, no accountability". This denigration of individual privacy seems unnecessary. If access to records held by mobile phone companies is required for law enforcement purposes, then the authorities would be able to obtain a warrant.

The issue of accessing mobile phone user information by authorities is not new. In 1997, there was an outcry by privacy and civil liberty groups upon the revelation that NSW police where monitoring mobile phone users without their consent or knowledge. With the help of mobile phone companies, the police were tracking criminal suspects through the triangulation signals sent to the nearest base station. Police protocol required officers to obtain written approval from their superiors and a court warrant before tracking the position of individuals. Although a useful investigative tool, this activity is open to abuse and raises serious questions of breach of privacy laws.

## BENEFITS

Tracking technology does have utility for society and the user. One of the primary arguments in favour of the use of tracking technology is that it enables people to feel safe. There is some comfort to be derived from the knowledge that someone can locate you if the need arises. Undoubtedly, tracking technology is an enormous benefit to rescue workers and law enforcement officials. Mobile phone users can be located even if the individual is unsure or incapable of stating their whereabouts. This advantage was evident in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Centre where rescue workers used mobile phone triangulation in the search for survivors. In Australia, Emergency Services often use triangulation as a tool to track injured and lost bushwalkers.

The United States Federal Communications Commission ("USFCC") have recognised the safety benefits of tracking technology. Late last year the USFCC ordered mobile-phone companies to incorporate tracking technology into mobile phones so as to enable law enforcement agents and emergency services to track the location of 911-mobile phone calls. By 2005, 95% of all mobile phones must have the 911-tracking technology installed.

However, the effectiveness of tracking technology in locating an injured or missing person is limited by its reliance on there being base stations/network antenna in close proximity to the person. Where there are long distances between base stations, such as in the Australian bush, it is near impossible to track the location of the person with any precision.

## RISKS

### (a) Loss of Privacy

'Privacy' and its counterpart 'surveillance' are key sociological issues. To an extent, enjoying a right to 'privacy' is fundamental to living in a free, democratic environment. The safety that comes in enabling people to find you when you are lost or hurt, means that people can also find you when you don't want to be found. It is possible that someone with criminal intent, such as a stalker could use tracking technology to locate their victim. Personal, but innocent activities such as attending mass on the weekend, or visiting someone in hospital may also be revealed. Similarly, the location of people who are on confidential government or corporate business may be disclosed with significant consequences. One must wonder whether the fundamental loss of privacy arising from this technology may be too high a price to pay.

### (b) Corporate Marketing Power

The marketable nature of the information gathered by tracking technology, poses great risks to our privacy. When collated, this data will disclose such things as where we shop and at what time. Even on 'stand-buy' our mobile phones relay our location to mobile phone towers. This is vital information for businesses. Marketing can be directly tailored to individuals and advertisements sent to mobile phones when the user is in the general vicinity of the organisation. Once permitted, it would only be a matter of time before every business used tracking technology as part of their marketing campaign.

The combination of tracking technology and caller ID may impact on the quality and fairness of phone sales and consumer enquiry numbers. It has been revealed that in the US, some corporations use caller ID to prioritise callers according to the suburb they are calling from. This enables the corporation to speak to prima facie wealthy customers first, thus maximising sales. Not only may this conduct amount to a breach of privacy laws, but it is a form of discrimination.

In defence of corporations, it is argued that consumer data derived from information about the location of mobile phone users would help to ensure that customer demands and capacity are met. However, one must ask whom the collection of such personal information and consequently the denegation of privacy really benefits.

## PRIVACY IMPLICATIONS

Given that this information, when coupled with the users name, may be considered 'personal information' organisations handling this information must comply with the Act and the NPPs or the IPPs.

Under the NPP 1 and IPP 1 information must only be collected if it is necessary for one or more of the organisation's functions and must be collected by lawful and fair means. As it stands, it is questionable whether the collection (particularly by an organisation other than a mobile phone company) of location data by way of tracking technology would be considered to be by 'fair' means. There is no evidence that mobile phone companies presently give collection statements to individuals as required under NPP1.3 or indeed that the individual is even aware that such information is collected, recorded and used.

In addition, an organisation must not use or disclose this information for a purpose other than the primary purpose of collection: NPP 2; IPP2. If mobile phone companies collect this information for the purposes of billing, they are prevented from selling this information for profit without consent from the individual. Such information may be disclosed where it is necessary to prevent or lessen an imminent threat to an individual's life, health or safety or for the prevention, investigation, prosecution or punishment of criminal offences.

Furthermore, organisations collecting personal information are required under NPP 4 and IPP 4 to ensure the security of this information. Given the prevalence of data mining and cybercrime, maintaining the security of such marketable information may be difficult.

## CONCLUSION

The collection use and storage of information detailing the location of mobile phone users has significant privacy implications. There is no doubt that in Australia there is a myriad of privacy laws and principles in place to protect the use and misuse of personal information. However, given the global nature of technology today, and the marketable nature of this type of information, one must question whether such laws will be effective in controlling the handling of personal information gathered by tracking technology.

*The views expressed in this article are those of the author and not necessarily those of the firm or its clients.*

***Rebecca Sharman is a Solicitor in the Information, Communications and Technology practice at the Sydney office of PricewaterhouseCoopers Legal.***

The Communications Law Bulletin is the journal of the Communications and Media Law Association (CAMLA) which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

## Contributions and 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 on disk and comments should be forwarded to:*

**Niranjan Arasaratnam**
**c/- Allens Arthur Robinson**
**Level 27, Stock Excange Centre, 530 Collins Street**
**MELBOURNE VIC 3000**
**Tel: +613 9613 8062**
**Fax: +612 9614 4661**
**email:**
**niranjan.arasaratnam@aar.com.au**

**or**

**Shane Barber**
**c/-PricewaterhouseCoopers Legal**
**Level 10, Tower 2**
**Darling Park**
**201 Sussex Street**
**SYDNEY NSW 2000**
**Tel: +612 8266 6787**
**Fax: +612 8266 6999**
**email:**
**shane.barber@pwclegal.com.au**

## Communications and Media Law Association

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 telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- defamation
- privacy
- advertising
- telecommunications
- contempt
- copyright
- film law
- freedom of information
- broadcasting
- censorship
- information technology
- 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.

### CAMLA Website

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

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:

- Ordinary membership $110.00 (includes GST)
- Corporate membership $495.00 (includes GST)
  (list names of individuals, maximum of 5)
- Student membership $38.50 (includes GST)
  (please provide photocopy of student card - full time undergraduate students only)
- Subscription without membership $110.00 (includes GST)
  (library subscribers may obtain extra copies for $10.00 each plus GST and handling)

Signature .....