Communications LAW B·U·L·L·E·T·I·N

THE OFFICIAL PUBLICATION OF THE COMMUNICATIONS AND MEDIA LAW ASSOCIATION (CAMLA)

Print Post Approved PP: 234093/00011 EDITED BY ANDREW LAMBERT AND JASON MACARTHUR Winter 1997 (Vol 16 No 2)

The Supreme Court's Ruling on the Communications Decency Act: A Victory for Free Speech

John Corker and Pauline Sala examine the recent US Supreme Court decision in Reno, Attorney General of the United States, et al v American Civil Liberties Union et al.

The Supreme Court on 26 June 1997 ruled for the first time that the Internet is fully protected by the First Amendment to the US Constitution. In upholding the earlier decision of the District Court for the Eastern District of Pennsylvania, the Supreme Court declared unconstitutional two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet in the *Communications Decency Act* of 1996 ("**CDA**") as a violation of both freedom of speech and personal privacy.

Judge Stewart Dalzell in the District Court stated in his decision:

> *"Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig."*

The District Court Decision

Two provisions of the CDA seeking to protect minors from harmful material on the Internet were challenged in this case. The first provision, described as the "indecent transmission" provision, prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age (section 223(a) of the CDA).

The second, known as the "patently offensive display" provision, prohibits the sending or displaying of patently offensive messages in a matter that is available to a person under 18 years of age (section 223(d) of the CDA). A number of plaintiffs filed suit challenging the constitutionality of these provisions.

The three judge District Court concluded that the terms "indecent" and "patently offensive" were too vague. They found that "the special attributes of Internet communication", with regard to the application of the First Amendment, denies Congress the power to regulate the content of protected speech on the Internet. The Court unanimously entered a preliminary injunction against both challenged provisions. However, the Court preserved the Government's right to investigate and prosecute for breaches of certain criminal provisions dealing with obscenity and child pornography.

The Government appealed to the Supreme Court under the CDA's special review provisions.

The Supreme Court Decision

The Supreme Court affirmed the judgment of the District Court and accepted the conclusion that :

> *"the CDA places an unacceptably heavy burden on protected speech, and that the defences do not constitute the sort of "narrow tailoring" that will save on otherwise patently invalid unconstitutional provision."*

Absence of Regulatory Precision

The Supreme Court accepted the first argument that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. Although the Government has an interest in protecting children from potentially harmful materials it held that the CDA pursues

INSIDE THIS ISSUE

CONTENTS

The Supreme Court's Ruling *(continued from page 1)*

that interest by suppressing a large amount of speech that adults have a constitutional right to send or receive. The Government may not:

> *"reduce the adult population...to...only what is fit for children".*

Further, the Supreme Court objected to the fact that the CDA:

> *"does not allow parents to consent to their children's use of restricted materials,"*

and the fact that it:

> *"omits any requirement that 'patently offensive' materials lack socially redeeming value."*

In fact, the Supreme Court stated that the general, undefined terms "indecent" and "patently offensive" cover large amounts of non pornographic material with serious educational or other value. It was argued that possible alternatives, such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into home, were the appropriate way to approach this issue.

In a dissenting opinion Justice O'Connor stated:

> *"the Communications Decency Act of 1996 is little more than an attempt by Congress to create "adult zones" on the Internet. The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if*
>
> *(i) it does not unduly restrict adult access to the material; and*
>
> *(ii) minors have no First Amendment right to read or view the banned material.*
>
> *As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecent transmission" fail to adhere to the first of these limiting principles by restricting adults' access to the protected materials in certain circumstances."*

Internet as a Unique Medium

The District Court's second argument was that the Internet is a unique medium different from television or radio and holds an enormous opportunity as a global market place of ideas and a powerful new engine of commerce.

> *"Neither before nor after the enactment of the CDA have the vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry."*

The District Court presumed that Government regulation will undermine the substantive, speech enhancing

benefits that have flowed from the Internet and will:

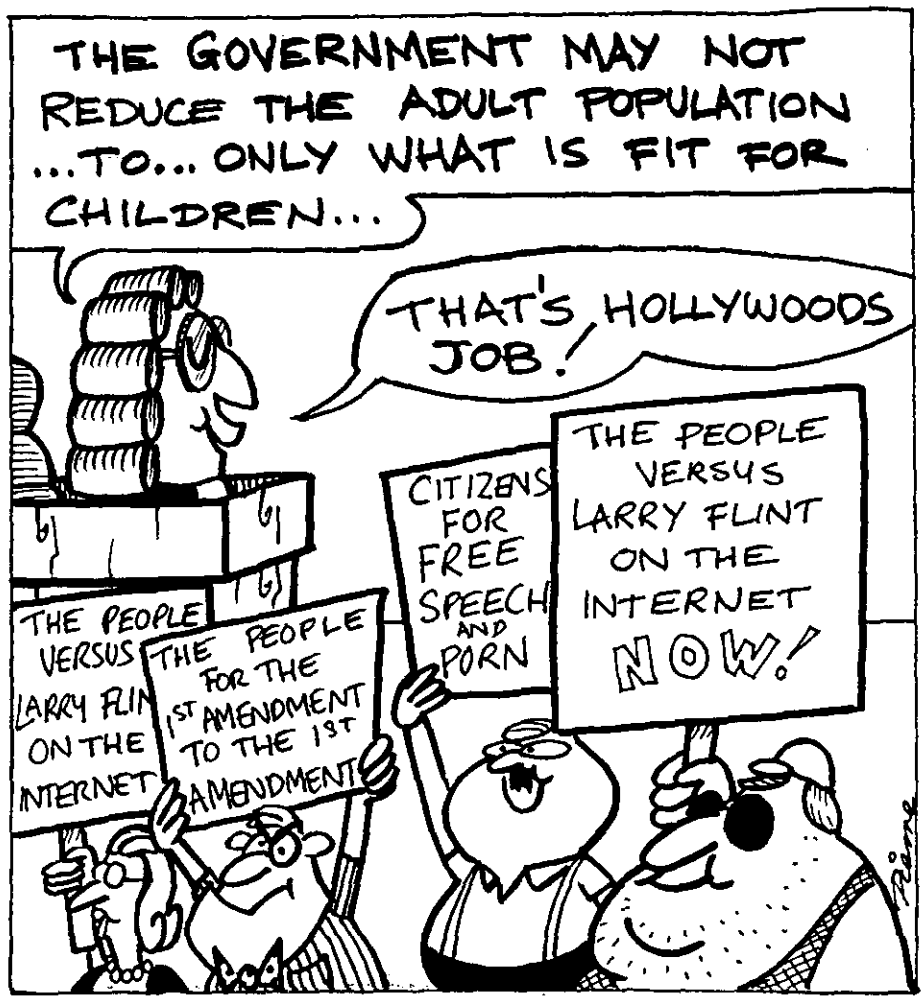
> *"threaten to torch a large segment of the Internet community."*

Judge Stewart Dalzell in the District Court wrote in part:

> *"If the goal of our First Amendment jurisprudence is the 'individual dignity and choice' that arises from 'putting the decision as to what views shall be voiced largely into the hands of each of us', then we should be specially vigilant in preventing content-based regulation of a medium that every minute allows individual citizens actually to make those decisions."*

The Supreme Court accepted this approach and rejected the Government's argument that availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.

John Corker is a legal officer and Pauline Sala is a legal assistant at the Australian Broadcasting Authority.



Self-regulation v. Censorship – ISPs & Internet Content Legislation in Australia

Andrew Lambert looks at the differing approaches taken at a State and Federal level with regard to the censorship of on-line content and some of the implications for Internet Service Providers.

Internet enthusiasts may argue the intrinsic value of free expression and the benefits of the free flow of information. However, this is not nearly as newsworthy as the idea of technologically literate kids surfing an Internet awash with pornography, neo-Nazis, paedophiles and bomb-making recipes. Media focus on the potential for the Internet to expose minors to harmful or inappropriate material has understandably led to concern in the community.

Politicians at a State and Territory level in Australia, responding to the imperative of such media attention, have taken an interventionist approach and have moved to censor content on the Internet. The Federal Government has been more reluctant to regulate on-line services, preferring to promote industry self-regulation and to refer specific issues, including copyright, to a variety of advisory bodies. The past few years have seen a profusion of Government enquiries relating to Cyberspace issues.

The most important has been the *Investigation Into the Content of On-line Services* by the Australian Broadcasting Authority (**"ABA"**) released on 30 June 1996 (the **"Report"**). This seems to have been adopted by the Federal Government as its preferred approach (discussed below). This has not prevented Victoria, Western Australia and the Northern Territory passing specific laws relating to content on the Internet.

State and Territory moves for On-line Censorship Laws

Recently there have been concerted moves by various States and Territories to introduce specific criminal offence provisions in relation to on-line content in Australia, which have attempted to co-ordinate their legislative response through the forum of the Standing Committee of Attorneys General ("SCAG"). However, there is some doubt as to whether the States and Territories actually have the power to do so given

that section 51(v) of the *Constitution* has been held to reserve the power to regulate communications of all kinds to the Commonwealth.

In 1996 SCAG proposed the development of model criminal offence provisions which would be introduced in a co-operative scheme between the States and Territories.

The New South Wales Parliamentary Counsel's Office drafted a discussion draft of criminal offences ("**Model Offence Provisions**") at the request of Ministers in charge of censorship in the various States and Territories following SCAG discussions.

The draft Model Offence Provisions proposed to make it an offence to send, receive, permit access to or retrieve "objectionable material" through an "on-line service". The provisions were subject to considerable criticism by the on-line services industry on the basis that they were generally unworkable. Although ostensibly designed to catch people who introduce offensive material on-line they effectively shifted criminal liability onto on-line service providers.

Phillip Argy of the Australian Computer Society commented that the Model Offence Provisions were the equivalent of making:

> *"Australia Post liable for carrying objectionable material inside sealed envelopes, Telstra liable for what people say on the telephone, local councils liable for what the public puts on community bulletin boards, shopping centre owners liable for what shopkeepers do in their shops and everyone criminally liable for the contents of unsolicited mail they receive".*[1]

Much to the relief of on-line service providers ("**ISPs**") the introduction of the Model Offence Provisions was postponed at the meeting of SCAG on 11 July 1996 following the release of the findings of the ABA Report. However on 9 July 1997 the annual meeting of SCAG announced that they may revive the project of drafting uniform national censorship legislation to deal with on-line services.

The ABA Report

Fortunately for the on-line community in Australia and ISPs in particular, the ABA Report seems to have forestalled any further cooperative legislative activity by SCAG and the States and Territories.

The key elements of the Report were:

(1) that the most appropriate approach to the regulation of on-line services content is a self-regulatory approach based on ISP industry codes of practice;

(2) the identification of matters which should be included in codes of practice for ISPs, which provide appropriate community safeguards, including complaints handling procedures;

(3) the registration by the ABA of such codes of practice, developed by ISPs after a process of public consultation; and

(4) the monitoring of the codes of practice and their effectiveness by the ABA.

The ABA recommended that compliance with any applicable industry code of practice should be provide a defence to an ISP in any prosecution under any State or Territory censorship laws, where such industry codes of practice were registered by the ABA. This was to occur as part of a co-ordinated regulatory and enforcement strategy applicable to the on-line industry.

The Report recommends that a complaints handling regime should be developed specifically for on-line services.

A range of matters which ISPs need to include in their codes of practice were identified including age verification procedures intended to limit the holding of an open line account to persons over the age of 18 to prevent children's access to open on-line services without adult supervision. Reasonable procedures to deal with objectionable material are to be adopted including practical steps which can be taken in respect of objectionable material once an ISP was made aware of that material. However, the ABA recognised that in some circumstances the measures which ISPs could take in relation to this material were limited.

In considering strategies to limit children's access to material which is unsuitable for them, the ABA offered encouragement for the Platform for Internet Content Selection ("**PICS**") which is an Internet protocol which can support the labelling of Internet content. This allows content providers to rate their web pages and for third parties to rate pages on the basis of a preset criteria. Parents or educational facilities can use this to screen access to unclassified pages or to pages with a rating which they consider inappropriate for their children or students. Parents can rely on self-classification by content providers according to this protocol or in accordance with a third party classifier whose moral viewpoint they agree with.

Other software is available which blocks access to sites which are based on PICS, including Cyber Patrol, Safe Serve, Net Shepherd and Net Nanny. They are combinations of filter software and labelling schemes for sites which provide parents and educational institutions with periodic notifications of problem sites.

The Report was widely praised in the on-line community and by ISPs. Since its release last June a number of Internet industry associations have commenced the process of drafting codes of practice which aim to meet the requirements of the ABA including:

- the Internet Industry Association of Australia;
- the Committee of University Directors of Information Technology; and
- the EROS Foundation.

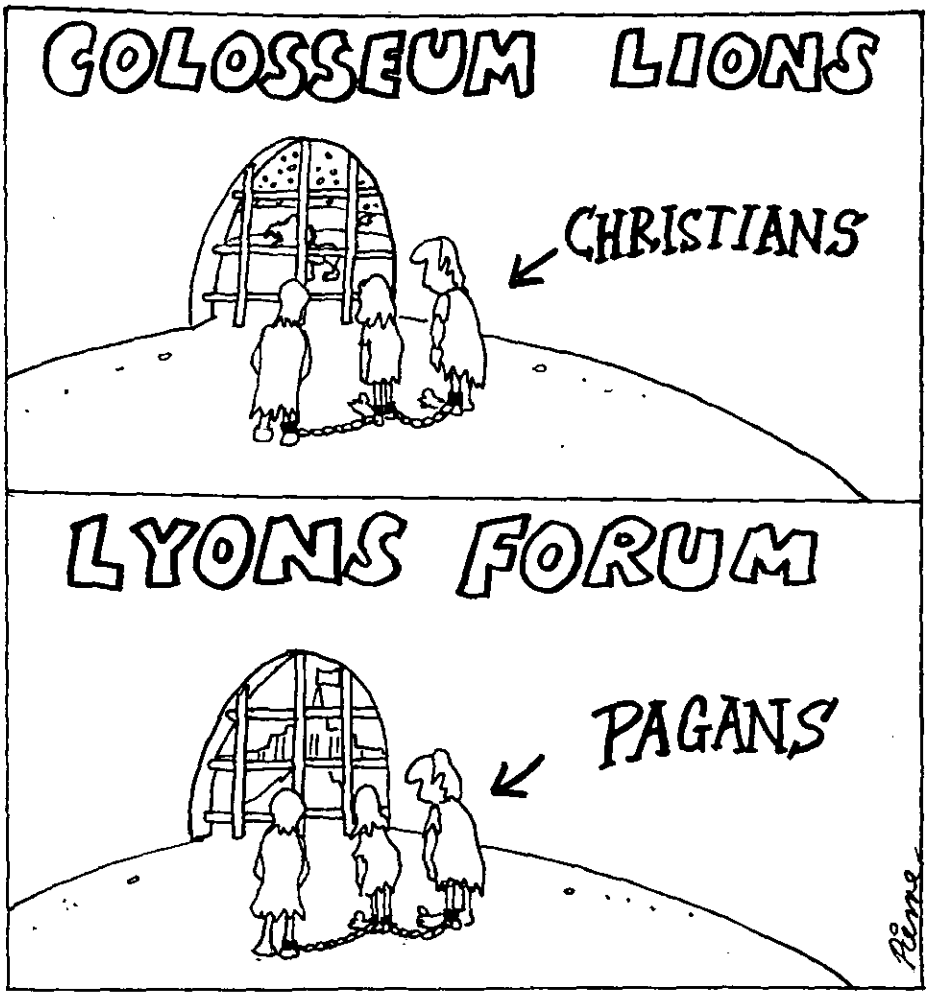
The Senate Committee Report

Just when the Cyberspace and its denizens in Australia were breathing a collective sigh of relief after the ABA Report (and the US Supreme Court's upholding of the US District Court for the Eastern District of Pennsylvania's decision in *Reno v ACLU*)[2], the Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technology (the "**Committee**")[3] delivered its report in June 1997. Deeply concerned with community moral standards, the Committee represents the other end of the spectrum on theories of the appropriate way of controlling on-line content to those of the ABA. Its recommendations included:

(1) fines of up to $100,000 per offence for the electronic transfer of pornographic or other "offensive material";[4]

(2) that on-line service providers be held responsible for on-line material;[5]

(3) that all States and Territories amend their classification and



censorship legislation to make it an offence to transmit objectionable material and to cover the transmission of material unsuitable for minors through computer on-line services, in a uniform manner;[6] and

(4) that specially designated units of State and Territory police forces should conduct random on-line checks to detect illegal activity.[7]

Federal Government Policy

However, the Federal Government appears to be following the path recommended by the ABA Report. On 15 July 1997 the Minister for Communication and the Arts, Senator Richard Alston, and the Attorney General, Mr Daryl Williams, announced principles for a national approach to regulate the content of the Internet based on the ABA's Report and on-going industry consultation.

The framework will be based on industry-developed codes of practice which will be supported by relevant amendments to the *Broadcasting Services Act* 1992 ("BSA"). The principal elements of the Commonwealth's approach include:

(1) facilitating the establishment of on-line industry codes of practice, incorporating an "effective, appropriate and fast complaints procedure";

(2) pursuing the development of international collaborative arrangements, such as PICS, industry codes of practice and industry forums;

(3) encouraging greater community awareness and fostering education programs; and

(4) encouraging the States and Territories to adopt an approach which is supportive of Australia's industry-based scheme, through both SCAG and the new "On-line Government Council".

The ABA will be the industry regulator to implement and monitor the national scheme. The BSA will be amended to provide the on-going authority for the ABA to work with the industry in developing codes of practice and as the industry co-ordinating body within the Federal Government.

The proposed arrangements recognised that ISPs were often not in a position to be aware of all material transmitted through their service and cannot be held responsible in every case for material they have not created. ISPs would meet their obligations by complying with industry codes of practice and acting quickly to resolve complaints.

Existing State and Territory Legislation relating to On-line Content

Victoria, Western Australia and the Northern Territory have all passed legislation directed at on-line content, either prior to or subsequent to the ABA Report. Western Australia and the Northern Territory's legislation was based on the discredited Model Offence Provisions.

The problem with all three pieces of legislation arises from determining where a breach is said to have occurred. Is it where the material is "transmitted" (uploaded on to the Internet) or where it was downloaded? This legislation has no extra-territorial effect and cannot prevent the transmission of such material into Victoria, Western Australia and the Northern Territory from other Australian jurisdictions and from outside Australia, if such material is legal in those jurisdictions. Serious questions about conflict of Australian law would arise should the relevant Police attempt to prosecute ISPs who intentionally or unintentionally provided access to material which is prohibited under local laws from servers located outside the jurisdiction.

The Western Australian and Northern Territory legislation create offences of transmitting "objectionable material" or "restricted material" to a minor or making restricted material available to a minor. The legislation does not define "transmit" but their definition of "computer services" is so wide it could catch any level of ISP (though not the telecoms carriers themselves). The breadth of the relevant definitions in the Western Australian and Northern Territory legislation for "computer service" would also apply the prohibitions on the transmission of "objectionable" or "restricted" material to e-mail.

The problem with this legislation as enacted is that it creates a strict liability offence placing the onus on ISPs to establish a defence. The Victorian act is different in that the offence is that of "knowingly" creating, publishing, transmitting or making available on-line objectionable material or material

unsuitable for minors, the onus being upon the prosecution to prove the element of knowledge.

The Northern Territory and Western Australian legislation assumes that on-line service providers are exactly aware of what is flowing across their networks and who exactly is accessing all relevant information, including the content of e-mail messages.

None of the means and protocols for accessing information on-line - e-mail, list servers, browsers, web-crawlers, search engines, indexes, bulletin boards, news groups, chat lines etc. - can effectively track the millions of users and screen out those under 18. ISPs could possibly age verify their own Internet subscribers but do not have the technical or human resources to control or even monitor the content of their subscriber's websites and communications in anything more than a random fashion. Nor can they be certain of preventing minors accessing materials on the Internet through the subscribers' terminals, whatever PIN or restrictive identification processes were adopted.

Other problems with the Western Australian and Northern Territory legislation are their definitions. The definitions of "objectionable material" includes by reference to material classified "RC" under the *Classification (Publications, Films and Computer Games) Act* 1995 (Cth) or that would if classified be so classified. This raises a question of how a person could be found to have knowledge of how unclassified material would be classified when the classification structure on which it is based is a subjective guideline. It may be difficult for a prosecution to prove the necessary criminal intent in respect of material that has not been classified by the Office of Film and Literature Classification (as is the case of virtually all material on the Internet).[8]

However, this may not be of much comfort with potential penalties for ISPs of up to $15,000 and 18 months imprisonment for individuals and up to $75,000 in other cases for the transmission of "objectionable material" by its users of which it had no actual knowledge. A more likely course of action is that large ISPs may simply avoid establishing their servers or Internet business operations in Western Australia or the Northern Territory.

Conclusion

The approaches adopted by the Federal Government and the States and Territories reflect the differing regulatory models of content specific and content neutral regulation.

The Senate Committee clearly has an agenda in imposing its moral strictures on a new medium the reality of which they do not understand and the primary feature of which - the free expression of ideas - they are profoundly hostile to. State and Territory politicians have responded to the spectre of Net pornography conjured by media reports with a knee-jerk regulatory response. Together these groups have attempted to apply traditional censorship laws developed to control content on the print and broadcast media to the Internet. Chasing headlines and sound bites is no way to draft policy and the ill-conceived Model Offence Provisions and the Western Australian and Northern Territory legislation it influenced are the result.

It is clear that applying censorship standards based on film and broadcasting content regulations to ISPs as if they were newspaper publishers or TV stations is inappropriate. However, merely treating them as a conduit akin to a telecommunications carrier removes obligations which the ISPs which do exercise editorial control over content on their services should rightfully be subject to.

It may be that the Internet as a new medium of communications needs new regulatory paradigms to control the content which can be accessed in Cyberspace. ISPs must play their part in preventing transmission of criminal material (especially child pornography) and restricting the access of minors to unsuitable material. However, this burden cannot be totally moved by regulators onto one component of the Internet, as has been attempted in the Northern Territory and Western Australia.

Industry self-regulation seems to provide a regulatory stop-gap until legislators can become more familiar with the working realities of this new medium rather than the hyberbole which surrounds it. Industry self-regulation also provides a safe haven for ISPs from the liability stemming from some State and Territory legislation. Most importantly it provides a forum in which the industry may be able to determine the most appropriate regulatory mechanism to govern it.

Federal Government policy favouring this approach seems, for the moment, to have given ISPs and industry groups breathing space in which to do so and to prove that they can act responsibly. They would be well advised to take advantage of it before the opportunity is lost.

Unfortunately, until a more equitable distribution of legal responsibility is effected by regulators, ISPs would also be well warned to avoid establishing their operations in jurisdictions which assume they can control or are even aware of the content that their subscribers are accessing and uploading via their services.

Andrew Lambert is a lawyer with the Sydney office of Deacons Graham & James. The views expressed in this article are the author's own and do not necessarily represent those of Deacons Graham & James.

1 Argy, Phillip "Internet Censorship Proposals" hhp:/www.msj.com.au/argy/intreg1.htm1.

2 No. 96-511, 26 June 1997.

3 Committee members include Senators Brian Harradine and John Tierney.

4 Recommendation 4.

5 Recommendation 1.

6 Recommendation 8.

7 Recommendation 9.

8 Op. cit. Argy.

Victorian Internet Censorship Legislation – is it Constitutionally Valid?

Tracy Francis examines Victorian on-line censorship legislation and questions its constitutionality in light of the High Court decision in *Lange v the ABC*

By the year 1999 it is estimated that there will be 200 million Internet users globally. The Internet is a decentralised computer network initially developed for the military. Today this self-maintaining network is a global infrastructure for communications and information services of unprecedented scope, diversity and accessibility. However, much of the mainstream reaction to the Internet has been concern relating to the ease of access to pornographic and offensive materials, particularly by children.

Both Australian and international governments have responded to this concern with legislation censoring the Internet: Victoria, the Northern Territory and Western Australia have enacted legislation, as has the United States, China and Singapore. The New South Wales Parliamentary Counsel's Office has prepared a discussion draft of model legislations, and whilst this has been rejected for implementation at a national level, the status of this legislation for New South Wales remains unclear.

It is argued that censorship of the Internet is undesirable for two reasons. First, in seeking to protect children the overall diversity of the Internet will be reduced, and adults will not be able to access on-line materials they could easily buy in a newsagency. Second, it is technically unfeasible for Internet Service Providers to monitor the information they disseminate and to verify the age or users accessing their service. Consequently, to comply with the law many Internet Service Providers will be forced to shut down, again reducing diversity.

However undesirability does not necessarily equate with invalidity. This paper examines the *Classification (Publications, Films, and Computer Games) (Enforcement) Act* 1996 (Vic) (the "**Act**") in detail. It is submitted that on the basis of the most recent Australian case law certain provisions of the legislation could be challenged as an unconstitutional restriction on free speech. The recent American decision, *Reno v ACLU* supports this conclusion.

The Legislation

The Act was enacted in January 1996 as a response to widespread community concern about the availability of objectionable material and in particular child pornography on the Internet. The relevant provisions are sections 57 and 58.

Section 57

Section 57 is a blanket prohibition on the creation and dissemination of objectionable material through an on-line service. There are two defences provided:

> (1) where the defendant can prove on reasonable grounds that he/she believed the material was not objectionable; and
>
> (2) for a service provider where that person did not create or knowingly download that information.

The definition encompasses e-mail, newsgroups and bulletin boards, Internet Relay Chat and the World Wide Web in its scope. As a result, communications between consenting adults through a medium such as e-mail are restricted by this provision. This is contrary to the principle that adults should be able to read, hear and see what they want, provided in the Schedule to the Classification *(Publications, Films and Computer Games) Act* (Cth) 1995. Moreover, material which can be obtained at a newsagent could conceivably fall foul of these provisions. For example, articles describing in graphic detail clitorectomies performed in some parts of Africa could easily be considered to:

"describe(s)...cruelty...or abhorrent phenomena in a manner that is likely to cause offence to a reasonable adult".

These types of articles regularly appear in women's magazines such as *Elle* and *Marie Claire*.

Section 58

Increasingly strict provisions are made in relation to the publication or transmission of certain materials to minors of any age and minors of less than fifteen years old. There is a defence available for a person who contravenes the section where they either:

> (1) could not have reasonably known that the person to whom the material was published was a minor and they had taken reasonable steps to avoid contravention; or
>
> (2) where the defendant believed on reasonable grounds that the material was not unsuitable.

This defence is mirrored for the publication of material to minors of less than fifteen, and there is the added defence that the person believed on reasonable grounds that the guardian of the minor had consented.

The defence for on-line service providers in s 58 is more strict than for s 57. In s 57 a service provider is not guilty of the offence except where they create or knowingly download the prohibited material. According to s 58(3) and s 58(6), the provider is not guilty of the offence unless he or she

> *"knowingly publishes, transmits, or makes available for transmission...to a minor material unsuitable...".*

Implications

Enforcement of these provisions will significantly affect material available to adults. There is no effective way to determine the identity or age of a user who is accessing material through e-mail, newsgroups or chat rooms. In relation to the World Wide Web, only where the server is capable of processing Common Gateway Interface script ("**CGI**") is it possible to interrogate a user of a Web site. However, as the large commercial on-line services such as America On-line and Compuserve cannot process CGI

scripts content providers using these servers currently have no technology available to them.

In view of these facts, it will be difficult for content providers to show, in accordance with ss 58(2)(a) and 58(5)(b), that they have taken reasonable steps to avoid publication to a minor. The fact that they could not have known they were providing material for a minor will be irrelevant. In relation to service providers the defence becomes virtually useless. Most service providers will be aware that they are providing some "unsuitable" material, even if they are unaware exactly what sites are unsuitable. Therefore, they are providing an on-line information service whilst knowingly making available for transmission to a minor material unsuitable for minors.

To avoid criminal liability both content and service providers will be forced to provide only material suitable for the lowest common denominator - minors under 15. As a result, a large amount of information which is ordinarily available to adults would have to be withdrawn from the World Wide Web and diversity will be dramatically decreased.

The effect of these provisions is to limit content providers and on-line service providers to publishing materials that are suitable for minors under the age of 15. This is clearly unreasonable, and will involve the restriction of political speech. Examples that were given as contravening section 57, would also contravene s 58. The legal issue therefore is whether the regulation of political speech in this context is consistent with the implied constitutional freedom.

Lange V. ABC

Since *Nationwide News Pty Ltd v Wills and Australian Capital Television v the Commonwealth* (1991) 171 CLR 1 it has been clear that the system of representative government guaranteed by ss 7 and 24 of the *Constitution* necessitate an implied constitutional freedom of expression in Australia. However, the scope of that freedom has been uncertain until recent times. In an attempt to remedy this uncertainty the High Court of Australia on 8 July 1997 delivered a joint judgment in the case of *Lange v Australian Broadcasting Corporation* (unreported, High Court, 8 July 1997.). The definition of "political discussion" and the scope of the freedom are fundamental to an analysis of the constitutionality of the Victorian legislation.

Content of "Political Discussion"

Prior to the *Lange* case there were a number of different formulations of the definition of "political" discussion. On the one hand, Chief Justice Mason and Justices Toohey and Gaudron took an interpretation of the freedom so broad as to include the discussion of activities that have become the subject of public debate where a link can be established with ensuring the efficacious working of democracy. On the other hand, Justice McHugh limited the freedom to a right to convey and receive opinion, arguments and information concerning matters intended or likely to affect voting within the election period. Justices Deane and Brennan took a middle ground allowing communications amongst citizens about matters relevant to the exercise and discharge of governmental functions and power on their behalf. Justice Dawson, who, prior to *Langer v the Commonwealth* (1996) 70 ALJR 176 held that the implied freedom was only in respect of representative government rather than in respect of communication, in that case felt compelled by the weight of authority to accept a freedom of communication and in rejecting the legislation in question referred to Mason CJ, Toohey and Gaudron JJ's view.

The benefit of the *Lange v ABC* case is that it provides a united statement as to what constitutes political expression. The judgment states that the freedom encompasses:

> *"communications concerning political or government matters between the electors and the elected representatives, between the electors and the candidates for election and between the electors themselves,"*

enabling those people to exercise a free and informed choice as electors. It is now clear that the freedom is not just limited to the election period - according to the Court, most of the matters necessary to make an informed choice will occur during the period between holding one election and calling another.

Looking to the Victorian legislation it is clear that material which is political may also be "unsuitable" or "objectionable". For example, a vehement attack in extremely colourful language, for example on the policies of the One Nation party, is clearly a communication relevant to a free and informed choice as an elector, but could also easily be a publication that

> *"describes crime... in a manner that is likely to cause offence to a reasonable adult".*

Similarly, photographs published on the Internet showing the results of heroin addiction for the purpose of criticising the Federal Government for failure to deal with the problem of importation and supply of heroin could easily fall foul of the Victorian legislation. Thus, some material prohibited by the legislation will also be political.

The Extent of the Implied Freedom of Speech

However, it is clear that the freedom is not absolute. It is limited by the text of the *Constitution* and it is limited in that legislation which impinges on the freedom may, nevertheless, be valid in certain circumstances.

Textual Limitations

The *Lange v the ABC* case unequivocally affirms the limitations of the implied freedom, and is at pains to emphasise that the freedom is not a personal right. In quoting Justice Brennan's statement in *Cunliffe v the Commonwealth* the judgment says,

> *"the implication is negative in nature: it invalidates laws and consequently creates an area of immunity from legal control, particularly legislative control."*

The point is that the implied freedom extends only so far as required by sections 7, 24, 64 and 128 of the *Constitution*. The Court says that insofar as statements in earlier cases appear contradictory, they should be understood as purporting to give effect only to what is inherent in the text and structure of the *Constitution*.

It is important to keep in mind that political speech will have to be relevant to the Federal arena in order to benefit from the implied freedom. In discussing the defamation defence of qualified privilege, the Court makes it clear that speech concerning, for example the United Nations or other countries, where it does not illuminate the choice for electors in an Australian Federal election, will not be protected by the freedom. It is submitted however, that discussions in relation to State politics would almost always be protected from legislation for the reason that the overlap of, at the very least, the political parties, will make it relevant to the federal arena.

Freedom Burdened but Legislation Still Valid

Nor is the restriction on legislative power absolute. This was clear even before the decision in *Lange v the ABC*. For example, in the *Langer v the Commonwealth* case a majority of the Court held that although the legislation in question burdened the freedom it was valid because it was appropriate and adapted to a legitimate legislative purpose. *Lange v the ABC* clears up the confusion in prior cases over the exact wording of the test for the validity of legislation which contravenes the freedom.

The test comprises two questions. First, does the law effectively burden freedom of communication about government or political matters, either in terms of its operation? Second, if the law does effectively burden that communication, is the law reasonably and appropriately adapted to serve a legitimate end the fulfilment of which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government and the procedure prescribed by section 128 for submitting a proposed amendment of the *Constitution* to the people?

Application to the Victorian Act

It is clear from the discussion at 2A above that the Victorian legislation burdens the freedom of communication. In applying the second limb of the test, few people would argue that protection of our children from obscene and pornographic materials is desirable and compatible with representative government. The crux of the matter is whether the Victorian legislation is reasonably and appropriately adapted to that purpose.

Recent media hysteria surrounding the Internet has alleged that it is rife with pornography and is a terrorist breeding ground. However, it is submitted that the range of available software applications which more effectively censor the Internet, in a less restrictive manner, means that the Victorian provisions cannot be regarded as reasonably appropriate and adapted to the legislative end.

Programs such as "Surfwatch" and "Net Nanny" and services such as the PICS rating service allow parents to evaluate material available on the Internet, and regulate such material by password. In this way parents are able to decide what they believe their children are old enough to have access to. As the holder of the password key, their own access to material would be unrestricted. The value of these services was recognised in the recent Australian Broadcasting Authority report, *Investigation Into the Content of On-Line Services* which stated:

> *"(A) new approach in limiting children's access is required. In this regard the ABA acknowledges that the most effective controls can be applied by users."*

Furthermore, it is unlikely that Victorian legislation could be effective. As one commentator has argued,

> *"When the average school kid wants to find some pornography on the Web, they are not going to be concerned about 'buying Australian'".*

In this case, "buy Victorian" would be more appropriate, however the point remains the same. Users can easily subvert the legislation by gaining access through an interstate ISP. There is also the potential that offensive mail can be sent through "anonymous remailers" located off-shore, the result being that the material is untraceable.

In relation to services that are readily accessible by anyone (such as the World Wide Web), if there is a serious threat of enforcement content providers and on-line service providers will have to censor material transmitted or published on the Internet to leave only that which is suitable for minors of under 15 years. This clearly involves the censorship, albeit incidentally, of some political discussion. Given the alternatives available it is unlikely that the legislation can be considered reasonably appropriate and adapted.

American Authority

The application of American constitutional authority to Australia is limited by the differences of the principles embodied in their constitutions and the history of their adoption. In relation to freedom of speech the most obvious differences are that in Australia the freedom is implied, restricted to political speech, and was only discovered in the early 1990's. In contrast, the American freedom is a right rather than a prohibition, is expressly guaranteed by the First Amendment, is unrestricted on the face of the Constitution, and has been continuously legislated on since inception. However, the persuasiveness of American precedent has been noted in many cases, and in recent times has figured strongly in the High Court's consideration of the implied right to freedom of political speech. Commentators have recognised the fertility of American jurisprudence in relation to freedom of speech, and for the purposes of this essay the US is the only jurisdiction, to the knowledge of this author, where the superior court has considered the regulation of indecent or offensive material on the Internet.

In *Reno v ACLU* the Supreme Court affirmed the decision of the District Court of Eastern Pennsylvania in holding that sections 223(a)(1) and s 223(d) of *The Communications Decency Act* (the **"CDA"**) are unconstitutional. Section 223(a)(1)(b) created a criminal offence for anyone who, by means of a telecommunications device, knowingly, makes, creates or solicits, and initiates the transmission of any communication which is obscene or indecent, knowing that the recipient is under 18. Sub-section (2) provides that anyone who knowingly permits any telecommunications facility under his control to be used for any activity in paragraph (1) also be liable. Section 223(d) made it a criminal offence for anyone who uses an interactive computer to send to a specific person under 18, or to display in a manner available to a person under 18, any communication that is patently offensive as measured by contemporary community standards.

The constitutional challenge was grounded in a series of arguments. Those relevant for our purposes were that the law was unconstitutionally overbroad (thus criminalising protected speech) and unconstitutionally vague, making it difficult for individuals and organisations to comply.

In finding that the law fails the "least restrictive means" test the court found that the burden placed on adult speech was unacceptable as less restrictive means, such as software allowing parents to restrict access to material, were effective in achieving the legitimate end of the statute, the protection of children. Significantly, the court recognised that it was not technologically nor economically viable for providers of Internet services to screen recipients of information for age. They rejected credit card verification and adult password verification schemes as effectively unavailable to a substantial number of Internet service providers. Although the wording of the test is different to the "reasonably appropriate

and adapted" test in Australia, the concept is similar. Owing to the scope of the freedom in America more material would be restricted by the CDA than by the Victorian Act, but these findings of fact are valid worldwide. The point remains that there are more effective and less restrictive means of censoring the Internet.

Conclusion

The Internet is a medium with some special features. The barriers to entry are very low - anyone with a PC and a modem can become a content provider. The barriers are the same for content providers and those who access the content. As a result there is an extraordinary diversity of material on the Internet - all those who wish to speak have access, and there is a relative parity between speakers.

This accessibility means that material on the Internet is not always as sophisticated or as polished as that available from other media. However, as Justice Dalzell states in the CDA case at first instance:

> *"What achieved success was the very chaos the Internet is. The strength of the Internet is that chaos".*

By its very nature the Internet comes the closest to creating a "market place of ideas" that has yet been seen. For these reasons, censorship of the diverse viewpoints on the Internet is grossly undesirable.

The type of legislation that has been enacted in Victoria is entirely inappropriate for the Internet. In forcing ISPs to take a greater control over what they publish the costs associated with providing that service will be greatly increased. Providers will be severely affected, and as a result we can expect the diversity of content to be affected.

Fortunately, it appears that there is a strong argument that the Victorian legislation unconstitutionally restricts freedom of political expression. It is difficult to view the legislation as reasonably appropriate and adapted when there are technologically more effective solutions available.

Tracy Francis is a recent graduate in law from the University of NSW and has joined McKinsey & Co. A version of this paper was Highly Commended in the 1996 CAMLA Essay Prize.

Developing Media Industries of the Future? Telecommunications and the "New Media"

John Colette examines the way in which telcom, film and software companies are attempting to use old media concepts to exploit a new medium - and failing.

In the endless wait for the promised "information superhighway", there are no shortage of players eager to assume the role of developers for the information industries of the future. Despite the explosive growth of and interest in networked media technologies, particularly the Internet, it is unclear if these "media" have moved beyond the early adopters who champion their use, into the realm of a true "mass" medium.

What is certain, is that in what appears to be the latent business opportunity of the millennium, it is extremely difficult for companies to build substantial and profitable businesses around the new media. On one hand, looking to develop this market, are the existing telecommunication companies, whose principal experience is in the provision of engineering based services and the development of network infrastructure. Also jostling for centre stage are software companies who have experience in the development of computer software. These companies have assumed that it is a logical progression for their existing products to "dovetail" into online media.

Applying Old Models to a New Medium

What is overlooked, is that the development of an emerging media form requires a creative flair that is elusive, if not impossible to hothouse within the confines of a large, corporate entity. Previously it was assumed that film and video makers would make ideal candidates for the development of "interactive" entertainment, because they understood concepts like "storytelling". In hindsight, this is patently not true, as filmmakers make good films, and the successful products that are computer mediated "interactives" are games like Doom and Quake, which are the product of another sensibility altogether.

This is why the software companies, even with extremely deep pockets, will have difficulty in "colonising" these new electronic frontiers. People are attracted to the online environment because of the anarchic variety of content that is available to them - most of which is free. This is completely different to the products and services models upon which software and telecommunications companies have been built. The popular "chat" lines that are a big attraction of the proprietary AOL online service in the US, have their genesis in IRC (internet relay chat). In these environments, users type messages that are read by an entire group in a "chat room". This is an aspect of the medium which mimics telephony, as opposed to the "publishing and broadcasting" models characteristic of the world wide web. What is important to note here is that the "content" is provided by the medium's constituency themselves - it is the distributed nature of the network that makes online chat "work".

Technology Does Not Drive Demand

What stands in the way of a clear view of the possibilities and directions of the online medium is a curious form of "technological determinism" that plagues the rhetoric surrounding new, digital technologies. In a determinist view of technology, the argument goes that a technology is developed, and there is a follow on effect on the social fabric. An example of this is the notion that the invention of the steam engine "caused" the industrial revolution, which ignores the historical fact that the first steam engine was shown operating on a circular track a full "30 years before a working railway was built. Similarly, in the rush to develop the new media, all types of products for augmenting the online experience with video, streaming audio and other "traditional" media types are developed and demonstrated on an almost weekly basis. This continues despite the fact that at the very core of the internet is a "packet" based technology, completely unsuited to delivering streaming media like video. Even with the development of so called "broadband" services duplexed on Cable TV coaxial lines, the bandwidth may support low resolution, compressed video, but the switching technologies around the network generally will not. The need to imitate existing media, particularly television, seems to stem from an insecurity as to what online media really are - the early years of television similarly assumed the form of "radio with pictures" with a studio based format derived largely successful from the radio genre.

Factors in a Successful New Media Application

If the factors that create a good new media application are isolated, they can be broken into three broad categories: media, networking and processing.

Media is simply that - the variety of media types that may be bundled under the abused title "multimedia". Networking is the ability of an application to take advantage of the distributed nature of the Internet to access a potentially global range of media sources. Processing is the ability, at either side of a transaction, to create additional value through the ability of computers to process information, such as through a database. Most emerging applications that show promise offer all three of these features to some extent.

At present, the development of online media is moving past the initial stage of novelty and into a growing period of maturity. Success in this environment is often enjoyed by small enterprises, with low overheads, that have developed niche new media "brands", as opposed to the larger corporate entities that produce, at great expense, derivative "channels" based sites that attempt to create broad market appeal, and in so doing, produce little that is not available in other, existing media formats.

The possibility of providing mass "entertainment" on the internet is remote - on the network, things are interesting in their specificity, the extent to which they address micro constituencies, or in the way that they are useful to the user. In the current environment, the successful developers of new media content will be those who can deliver specialist media to an audience that actively seeks it, or in more broadly based applications, those that deliver context and use value for the content they provide.

John Colette is head of Digital Media at the Australian Film, Television and Radio School.

Electronic Commerce Today & Tomorrow

The following is an extract from the address by JoAnn Patrick-Ezzell, President, AT&T Online Services, 4 July 1997 to Tradegate and ECA members. It examines the likely future development of electronic commerce and the elements that drive and shape its evolution.

Forecasting the future is always difficult. I do believe, however, that the Internet is fundamentally changing how we communicate, how we collaborate, how we conduct commerce, and how we learn. This paper sets out a vision of the emerging electronic commerce environment and some of the requirements to enable its continued successful development.

Growth of the Internet and Electronic Commerce

The evolution of electronic commerce will be shaped, in large measure, by Internet-related developments.

Calculating and reporting on Internet statistics has become as commonplace as assessing the weather — and just about as accurate.

One of the better statistical measures of Internet growth is the number of Host Computers (a host computer is defined as a domain name that has an IP address associated with it— think of it as a computer connected to the Net).

From January 1996 to 1997, the number of Host Computers worldwide has grown by 70 percent to over 16 million. I would not be surprised if the *Network Wizards* survey to be released later this month pegs the July 1997 number of Host Computers at over 20 million.

In North America, the number of Host Computers in just one year had grown by 151%, totalling seven million. In the same period, the number of Host Computers in South America grew by 215%. Europe represented 37 percent of the total, with growth at 62%. Closer to home, the growth of Host Computers in Asia/Pacific was 154%. And second only to Japan, Australian Host Computers represented about one-third of the total in Asia/Pacific and the growth rate here was 66% for the past year.

The Internet is developing rapidly in Asia/Pacific, not surprisingly, as the region is home to so many of the world's semiconductor, disk drive, and PC factories. With about 2.7 million users, Australia is currently the most connected country in Asia/Pacific. The number of Internet users in Asia/Pacific is expected to exceed 50 million by the year 2000.

Today, there has also been unprecedented growth in electronic commerce as well. I believe the forecasts that electronic commerce will reach US$50 billion by the year 2000 are much too conservative.

In one survey published earlier this year by CommerceNet (an industry consortium) and Nielsen, the media-research firm, 73% of Internet users had used the web for shopping in one way or another in the past month.

Electronic Commerce – the Big Money

However, the big money is not in consumer shopping but in business-to-business commerce. The reason of course is that many business transactions are already conducted at a distance, whether by fax, telephone, post, or private network.

EDI has made the supply chains of businesses today far more efficient. Today, an estimated 95% of Fortune 1000 companies use EDI in one way or another.

I will highlight what I believe are the most significant ways the Internet will impact on these four components.

It's important to keep in mind that existing secure messaging systems, and notably EDI, will play a key role in the development of this emerging electronic commerce environment. What will change is the level of ubiquity and user-friendliness inherent in applications— if you will, the end of the "Tyranny of Distance."

By using Internet technology a business can enhance the flow of information within their operation and establish a one-to-one relationship with their customers. The back office can interact directly with employees, partners, suppliers, and customers, creating new synergies and opportunities. The store front can be reached by customers and monitored by managers, at anytime, from anywhere. And the consumer and end user can finally participate as an equal in the flow of information that is the lifeline of commerce.

It's true that before we reach this level of productivity and sophistication, there are some basic requirements that need to be met.

Requirements for Continuing Development of Electronic Commerce

I think one of the best salespeople of all time must have worked for AT&T, some 100 years ago. Can you imagine what it took to sell the first telephone? Think about it... who was the person going to call? Connectivity today is as critical to the success of electronic commerce as it was to our first customer. It follows, therefore, that ubiquitous and accessible communication infrastructure is indispensable to the adoption and implementation of electronic commerce.

Another requirement for electronic commerce is the economic readiness of the parties involved. Consumers must be able to afford the necessary technology and must have the means to stimulate the interest of businesses around the world. Businesses must also afford the technologies that will bring their operations into the information age.

And importantly, we will need to bridge the cultural gaps that separate us. We must find a way to overcome communication barriers.

Five years ago it would have been inconceivable to fulfill these requirements in the near future. The Internet is changing this.

PC Penetration and Teledensity

Let's take a look at telephone, television, computer, and wireless penetration. Australia has the highest percentage of

PC penetration and teledensity in Asia/Pacific. There are many countries in Asia/Pacific with low teledensity, however. The Philippines, Indonesia, the PRC, Thailand, and Malaysia have low telephone penetration, but relatively high TV penetration. This is an important characteristic that may enable them to overcome current infrastructure shortcomings as new access methods are developed.

Teledensity growth— the number of lines per person— in Asia is expected to jump 111%. And by the year 2000, the number of actual lines will more than double to 375 million.

To give an example of the enormous expansion, China is planning to install telephone lines at the rate each year equivalent to the size of a US Bell regional operating company. Or put another way, they'll duplicate Australia's entire national network every year. The projected teledensity growth rate in the US pales in comparison to the Pacific Rim— with a 15% growth opportunity expected by the year 2000.

Plans for the first fibre optic undersea telecom cable directly between the US and China were announced this year. The cable will increase capacity 16 fold— jumping from 5 to 80 gigabits per second. It will transmit more than one million simultaneous calls, higher than any undersea facility now in operation.

Overall, Asia/Pacific's cellular subscriber base is expected to exceed 70 million by the year 2000, quadrupling revenues to $50 billion.

And, one of the biggest changes over last year in the Asia/Pacific Internet market has been the building of Internet backbones. I'm pleased to say AT&T was at the forefront— building the first Internet backbone network in Asia/Pacific, linking Japan, Hong Kong, and Australia with connectivity back to the US.

The flexibility of digital technology allows information to become independent of the medium. WebTV, for example, broadens the Internet user base and integrates the computer with the television, and vice versa. For network computers recent technology breakthroughs range in significance from being able to carry a device with powerful information access capabilities in your pocket to slashing computer costs to under US$500. Cellular telephones are being applied to the Internet through companies such as Unwired Planet. Infrastructure solutions like these potentially make computers and networks available to many more people— to masses of people in Asia/Pacific and the world.

New Economic Models

As you know, Australia ranks in the top 10% in the world and fourth in Asia/Pacific in terms of per capita income— estimated to be US$21,000 this year. Obviously, an adequate income level is necessary in order to truly benefit from the breakthroughs in Internet technology and from the vast information resources available online. Much of the hardware needed to use the Internet to its fullest is still too expensive.

Just as there are new technologies to overcome infrastructure challenges, there are new economic models that may help bridge the affordability gap. For example, companies like Hotmail offer free email service by subsidizing it with advertising. This presents a new economic model. Businesses may choose to carry access costs previously charged to consumers in exchange for the chance to build a direct relationship with a customer.

In addition, the appliances used to access communication services need not be economically prohibitive. Take Diba for instance. Diba produces inexpensive appliances that perform basic Internet functions, such as browsing, e-mail and fax, in some cases by combining with common home appliances to minimize costs. For example, Diba Internet uses the television as a monitor. Inexpensive devices and access methods such as these will broaden the type, and number, of participants in the electronic commerce environment.

English Literacy

Cultural readiness is related to literacy since most information available on the Internet today is print based. I'm defining literacy here as the population over 15 years of age with the ability to read and write a short, simple statement about everyday life. Even with today's graphical Websites, for a user to manoeuvre online, he or she must be literate. Australia has one of the highest literacy rates in the world. High literacy rates enable most of the people of Australia to easily use the Internet related information available to them.

Apart from literacy, the language issue must be addressed in the development of the emerging electronic commerce environment. In most cases, up until now, to use most of the information available online, it is not enough for one to be literate— one must also be proficient in English. Here again, Australia has an advantage as a native English speaking country.

This requirement is also being addressed by technology. The development of real-time translation software allows users to communicate and access content in their own language. Many websites, such as our site in Japan, are available in more than one language. Providing multilingual content and access is an important part of bridging cultural differences worldwide. Australia's multi-cultural society and skilled multi-lingual workforce again is relevant to note.

Software such as Typhoon translates English content into passable Japanese. The sentence construction and idioms may not always be perfect, but users who don't read English at least have access to a passable translation of Website information. The need for multilingual usage goes further. Inability to conduct foreign language searches has traditionally hindered non-English readers from accessing foreign language Website information. Now multilingual search engines, such as Globepage, allow Chinese and other foreign language search queries.

Internet resources are useful in proportion to the number of people who can make use of the Online information. Multilingual access devices are broadening the user base by helping bridge language differences. Soon, users may be able to communicate and access Online content in any language, and this ability will tie all users together in a way we have never known before.

I see the aspects of Infrastructure, income, and culture I just talked about as key requirements to address in order for the emerging electronic commerce environment to grow.

Examples of Electronic Commerce in Action

As I mentioned at the outset, I'd like to share some examples of how the Internet is currently being used to enable electronic commerce. These examples give us an idea of how far we've come, and help us think about how much further we can go.

Ford and CustomBoard integrate the Internet into their entire business operation. The Australia Customs Service facilitates back office operations through EDI. ImageNet has set up a Store Front on the Internet, and Qantas and JAL provide the Consumer with online support.

CustomBoard, the American snowboard manufacturer, is an innovative example of a company that is integrating the Internet into the core of its business operations. CustomBoard uses its Website to automate the ordering process. Interested consumers provide information such as their desired board base and size. Customers can also email the company graphics they want on their snowboard. The customer information is then sent to the company's production department. Using this information, CustomBoard's snowboard crafting machines automatically build the board to customer specifications. From there, the finished product is shipped directly to the customer. There are virtually no inventory costs associated with this method of production. Although CustomBoard serves a niche market, it is a useful example of just how companies are currently using the Internet to improve the efficiency of their business.

The key feature of electronic commerce applications in the customs area is back office integration and the economies this brings. The integration of customs' in-house applications with the EDI messaging program is one side of the equation. The other is the potential for the many trading partners to automate their business systems.

Current levels of integration have improved the delivery of trade facilitation across many of the customs applications. The latest electronic commerce developments offer information services as well as transaction processing and address a wider range of potential applications extending from the present base through the extended commercial processes. There are great potential user benefits from these functions.

One of the great qualities of Internet enhanced electronic commerce is that in some cases the entire commerce transaction can occur online. ImageNet uses its Website to display and sell its photographic images. More interestingly, once a customer has made a purchase, ImageNet then allows the buyer to download the image as a high-resolution file.

Information transactions are just as integral to the emerging electronic commerce environment as transactions that involve the exchange of capital or goods. Qantas and JAL, for example, share information from their company databases with consumers, providing them with a valuable service.

Qantas provides worldwide flight locations information, from which users can put together their itineraries. Consumers can also access contact numbers for sales agents who can handle ticketing and information on destination hotels. Similarly, one of our customers in Japan, JAL, has a Website that provides information on public transportation to airports around the world. The site also lists flying regulations, such as acceptable luggage sizes and materials allowed on board. Information resources like these benefit both the consumer and the business. On the business side, Qantas and JAL save on staff requirements and time needed to provide this customer information.

There is so much potential for using the Internet to help improve electronic commerce. The examples I shared with you demonstrate current business uses, but in the future, new technologies, along with the same creativity and innovation, will enable even more powerful applications.

Technologies that will Drive More Complex and Powerful Applications

The transformation brought forth by the technology industry over the past 20 years, exemplified by the invention of the microprocessor and the advent of the PC, pale in comparison to the explosive and innovative growth of Internet technology. Five developments: information push technology, artificial intelligence, Internet telephony, electronic cash and Intranets, are among the exciting technologies driving change.

If we look at the unprecedented growth of the Internet in the last few years, there is no question about the critical role played by the introduction of the browser. This because to a great degree, the growth was driven by the explosion of the World Wide Web.

The Web, however, is not the Internet. It is part of the Internet, a part that has sprung to life around the browser. How much longer will the browser and the Web drive the growth and expansion of the Internet? I believe not much longer.

This is not to say that the 150 million web pages of today will not reach the 1 billion mark by the Year 2000. Websites will continue to grow but they will not be driven by browser technology alone. The next technology that will revolutionize the Internet is here and will soon be pushing its way onto desktops and televisions around the world.

Information push technology is what I believe will drive the Internet into the 21st Century. It is at the heart of what will drive different media and industries to converge on the Internet. Push technology combines aspects of the web with the qualities of broadcast media and this will no doubt create incredible opportunities.

One interesting technology driver is artificial intelligence. Intelligent agents will become critical as more and more information is pushed on to our desktops, laptops, palmtops, set top boxes and the myriad of devices that we use. Intelligent agents, which understand our individual needs and preferences, will filter information and help the content provider deliver the right stuff, in the right amount, to the right person, at the right time.

Among their many uses, intelligent agents will also be able to automate production level adjustments, and arrange for the efficient delivery of goods. Intelligent agents will be able to handle much of the work previously handled by people. Intelligent agents will also be our online assistants, helping us in handling our day to day tasks. For example, if an intelligent agent knew its "boss"— for example, a company, was interested in upgrading its employees' computers, it could search for and possibly purchase the best bargains from a hardware provider on its own, thus saving its "boss" money and time.

It's easy to see how Internet telephony can be a major catalyst for Internet adoption. The savings offered by Internet voice over IDD and LD will drive Internet use and in doing so open the way for other Internet applications. The enhanced features Internet telephony will provide, such as real-time data sharing and video capabilities, will also help improve communication in the electronic commerce environment.

The recent deregulation of the Australian telecommunications industry should encourage a new diversity of communications services such as Internet telephony. An example of Internet Telephony is AT&T's Project iA— iA stands for "Instant Answers". This is an

example of how toll-free services and web hosting can make it easier for businesses and consumers to conduct electronic commerce. Project iA is a two-way, agent-assisted transaction processing technology for the Internet. Users click on an icon to initiate a telephone conversation with a customer service agent. The agent can send images to a customer's screen to illustrate the products or services being discussed. Consumers will be able to get "instant answers" on demand and make secure credit card purchases. Businesses will benefit from a new sales channel and more completed transactions.

Methods of Payment

To make that next step in enabling consumers to easily use the Internet to conduct electronic commerce, new means of payment will evolve. One possibility is electronic cash— money in the form of electronic information that can be stored on a computer or on a plastic card with a microprocessor imbedded in it. Electronic cash can be moved around the world through the Internet or any other electronic medium.

Electronic cash lets the consumer pay the storefront directly, through an anonymous and secure connection, without having to go through an intermediary, such as a credit card company for verification. Electronic cash addresses two key issues that today inhibit the development of electronic commerce: security and anonymity.

However, I do agree with Jim Barksdale, Netscape's CEO, when he says he doesn't know of a dime that's been lost over the Internet. Executives at Visa International indicate that there is not a single properly documented case of fraud involving credit card numbers stolen over the Internet. Clearly, though, users need to become more confident in using credit cards and potentially electronic cash to make purchases over the Internet. The security exists to conduct these transactions safely, but this must be proven to the user.

One of the questions I'm often asked is: "Will the Internet become the environment for electronic commerce?" The Internet is a lot of things. My personal belief is the Internet is more important in what it enables and what it will evolve to than simply what it is today.

One of the keys to the future lies in the future of Intranets. Intranets use Internet technology, leverage the ubiquitous nature of the Internet, and address security requirements. By creating virtual private networks, user entrance is regulated. Such levels of security will encourage users and enable the electronic commerce environment to flourish.

In electronic commerce, many of these trends have been gathering force for years and are only now becoming obvious as they are harnessed to the explosive growth and global reach of the Internet. For all the attention, hype, and impact of the Internet to date, I think it's about to get even more exciting.

In reflecting on these technological trends it's clear that there exists a strong inter-relatedness and, in fact, interdependence. As these and other technologies develop, they fuel each other and will eventually create a critical mass effect that will catapult electronic commerce even further.

So, although the Internet can be thought of as a network of networks embracing software, hardware, and other technologies, it is more significantly a new mass medium, a catalyst for change— enabling new things never before imagined.

Using the Functionality of the Internet to Further Evolve Electronic Commerce

Whereas most technological innovations have taken five or even ten years to achieve significant scale, the Internet is impacting industries and even culture in time frames measured in months or a few years.

Speed has become everything in this business. Our challenge is to enable EDI and other systems and services to benefit from the flexibility and ubiquity of the Internet.

In terms of the technology, we need solutions which incorporate the ubiquity and economy of the Internet, the imagination and functionality of web development, and a secure transaction processing environment. At the organizational and institutional level it is of paramount importance that links between businesses, individuals, community groups are enhanced and function effectively - to the benefit of all parties.

JoAnn Patrick-Ezzell is the President of Online Services AT&T Asia/Pacific

Recent Cases on Advertisement of "Free" Items by Telecoms Operators

Dr Warren Pengilley looks at comparative advertising, the advertising of "free" items and what we can learn from recent cases on advertising by telecommunications companies

There has always been some contention in relation to comparative advertising tactics and in relation to what is meant by items advertised as "free". The telecommunications battles of recent times have thrown up some court cases which are illustrative of the problems involved and give useful law on these two subjects. The cases are *Australian Competition & Consumer Commission v Telstra Corporation Limited* [(1997) ATPR ¶ 41-540: Federal Court of Australia - Jenkinson J]; *Telstra Corporation Limited v Optus Communications Pty Limited* [(1997) ATPR ¶ 41-541: Federal Court of Australia - Merkel J]; and *Nationwide News Pty Limited v Australian Competition & Consumer Commission* [(1997) ATPR ¶ 41-543 - Full Federal Court of Australia]. The three cases are conveniently reported in virtually adjoining reports in the 1997 volume of the *Australian Trade Practices Reporter.*

It is intended here to deal with the principles which emerge from each of the cases.

Australian Competition & Consumer Commission ("ACCC") V Telstra Corporation Limited ("Telstra")

This was a proceeding for declaratory and injunctive relief.

Optus Communications Pty Limited ("Optus") announced in June 1996 the inception of its arrangements that a local telephone call service in Australia would be 20¢. At that time the generally applicable charge for each local call on Telstra's telephone service was 25¢.

Telstra subsequently made public statements in relation to the local costs made under a plan offered by Telstra to its customers and known as the Local Call Saver 15 Flexi-Plan ("CS15"). This plan provided as follows:-

- If customers made more than 2 local calls a day a discount of 15% applied which resulted in all local calls costing 21¢.

- If customers spent more than $15 per month (2 calls per day) all local calls above that attracted a 15% discount.

- Discounts were available on all local calls made under CS15.

- CS15 was available to all customers without limitation.

It was alleged that the representations were false in that:

- If customers made more than 2 local calls then the discount of 15% did not apply and this resulted in all local calls costing 21¢.

- If customers spent more than $15 per month (2 calls per day) all local calls above that did not attract the 15% discount.

Discounts were not available on all local calls made under CS15; and

- CS15 was not available to all customers without limitation.

In the particulars filed in the case, the ACCC set out the average calls made per day and the average call cost in a month. These varied significantly. Suffice it here to say that if an average of 2 calls were made per day, then the average call cost in a month was 25¢. If an average of 20 calls were made per day, the average call cost was 22.88¢. The lowest cost involved was that applicable to 13 calls per day and this cost was 21.81¢.

It was submitted by Counsel for the ACCC that statements made by Telstra executives along the lines set out above on radio and television were misleading or deceptive. This was because the Telstra executives stated that the basic price for a call for customers who spent more than $15 a month on Telstra's Flexi-Plan was 21¢ whereas the actual charges were not levied on this basis.

The court said that the executives involved had access to officers of Telstra who did have precise knowledge of the costing of the calls even if they themselves lacked such knowledge. Thus the failure of those executives to avoid engaging in misleading or deceptive conduct was "in the circumstances, deplorable".

Mr Justice Jenkinson stated that:

> *"Harm done by conduct of (the above) kind is not wholly undone by subsequent retraction and explanation and curial retribution. Among the multitude of customers misled by such conduct not a few are likely to remain unaware of the retraction and retribution."*

Accordingly, his Honour restrained Telstra (for a limited time only in view of the circumstances outlined in the judgment) from making a false or misleading representation on radio or television programmes in respect of the amount of any charge for a telecommunications service.

Lessons from the Case

A lesson from *ACCC v Telstra Corporation Limited* is a fairly simple one. This is that representations as to costs savings must be accurate in all respects. It seems as if the Telstra executives making claims on radio and television were not fully informed of the situation. However, this did not excuse them or Telstra. The executives involved had ready access to the true information or to those Telstra officers who knew the actual position. Obviously a claim that calls under the CS15 Flexi-Plan cost no more than 21¢ could not be other than misleading or deceptive when the cost of calls ranged from 25¢ to 21.81¢.

His Honour stated that:

> *"Under the exigencies which keen competition for the custom of a multitude of consumers imposes on the respondent it constantly resorts, as does its competitor Optus, to repetitive television advertisements marked less by information than by*

emotional stimulation. I would expect that the text of such advertisements would be carefully scrutinised by the respondent's advisers to ensure that no misleading conduct occurred."

Telstra V Optus

In this case, Optus was the defendant in proceedings brought by Telstra. Again, the issue was the cost of telephone calls.

Optus conducted a national television programme relating to its Optus guarantee and to the price of international telephone calls. Both the guarantee and the international cost of calls were part of a broad campaign of commercials designed to take advantage of the fact that Optus' standard international rates were cheaper than those of Telstra. The Optus guarantee had been developed as a means by which customers would be assured of saving on their total telephone bills and promised customers savings on their total long distance call bill compared with Telstra. Customers became entitled to the benefits of the guarantee once they signed an authority to change their long distance carrier. Optus compared its bills against Telstra's bills and guaranteed a credit to customer's account of twice the difference shown if the customer's account was lower with Telstra. As it turned out, although Optus' standard charges were cheaper than Telstra's standard charges, Telstra's range and variety of discounts available, including Telstra's Flexi-Plan, made price comparisons very difficult to make.

Telstra complained that in the Optus commercial, Optus had falsely represented that its prices for long distance and international calls were cheaper than Telstra's prices. Optus disputed that its representations were misleading or deceptive and claimed that its commercials were true.

The Decision

The Optus evidence was that the Telstra's complicated cost savings plans led to it being very difficult for customers to compare like with like. Billing by each carrier was on a periodic basis and compared the total billing for all telephone calls and services provided during the relevant period after taking into account the discounts to which particular customers were entitled. Optus said that its marketing campaign was focussed on the aggregate bill amount as opposed to individual call rates and the comparisons were made on this basis. Hence the Optus guarantee was developed as a means by which customers could be assured of "bottom line" savings that is, savings on the total bill.

Mr Justice Merkel characterised the case as one which raised the issue of whether a television advertisement which may or may not contain an inaccurate statement or representation when its visual, audio and written constituent parts are carefully considered, can nevertheless breach section 52 of the *Trade Practices Act* (covering misleading or deceptive conduct) because the impression its interacting constituent parts conveyed is misleading or deceptive or likely to mislead or deceive. Thus, for example, the international calls commercial raised two interrelated questions. The first was whether the example of "normal" rates which was given, whilst accurate in itself, was misleading in that the overall impression created by the commercial was that Optus offered cheaper rates generally for international calls. Clearly, said his Honour, the impression given by the advertisement was broader than the specific example given in the advertisement itself. The second issue was whether the failure to state that the comparison might not apply to customers using the Telstra Flexi-Plan made the commercial misleading.

The case was an application for an interlocutory injunction and thus the issues before the court were whether there was a serious question to be tried and whether the balance of convenience favoured the grant of an injunction.

His Honour held the following principles to be applicable as regards whether or not section 52 of the *Trade Practices Act* was breached:

- the advertising of Optus must be viewed in the context that it was on national television;

- the conduct of Optus must be viewed as a whole. It would be wrong to view words or acts alone which might be misleading or deceptive when, viewed in their overall context, they were not capable of misleading;

- it would not be right to select some words only and to ignore others which provided the context which gives meaning to particular words;

- under section 52, the importance of first impressions conveyed must be given considerable weight. However, balanced against this, a fairly robust approach must be called for when determining whether television commercials are false, misleading or deceptive. This is because the public is accustomed to the puffing of products in advertising. Although the class of persons likely to see the commercial is wide, it is inappropriate to make distinctions that are too fine and precise;

- one must look at the veracity of its message by reading it in context. One also needs to take into account the fact that many readers would not make a close study of the advertisement but would read it fleetingly and absorb its general thrust;

- a statement may be deceptive even if the constituent words may be literally or technically construed so as not to constitute a misrepresentation. The buying public does not weigh each word in an advertisement or a representation. It is important to ascertain the impression that is likely to be created upon the prospective purchaser;

- thus even though each sentence considered separately is true, the advertisement as a whole may be misleading because factors are omitted which should be mentioned or because the message is composed to highlight the appealing aspects.

His Honour, in his decision, cited a number of Australian court and United States decisions and commentaries to support each of the above propositions.

His Honour commented on the question of comparative advertising and, in this regard, made the following points:

- When a person produces a television commercial that not only boosts his own product but, as in this case, compares it critically with the product of another so that the latter is shown up in an unfavourable light by comparison, such advertiser ought to take particular care to ensure that statements are correct.

- In comparative advertising errors may have a greater potential to mislead consumers than statements made in ordinary advertising which may be perceived as mere "puffs".

- In particular cases, a "half-truth" may be misleading or deceptive. A comparison between goods or services may be rendered misleading by the

omission of material that would be necessary to render the comparison fair. An unfair comparison may, quite simply, because it is unfair, be misleading. It may mislead a consumer into thinking there is a basis for a choice where, in truth, there is not or that a choice may be made on grounds which are not truly valid.

His Honour cited a number of Australian court decisions for each of the above principles.

Applying the above principle to the Optus' advertisements, his Honour believed that the Optus message was:

- Optus guaranteed that its long distance telephone prices and consequently its bills were cheaper than Telstra's; and

- Optus would credit the customer with double the difference it was wrong.

His Honour found that implicit in that message was a representation by Optus that its long distance telephone prices were cheaper than Telstra's prices. However, Optus' own case accepted that a general price comparison cannot be fairly or accurately made. The offer by Optus to credit double the difference between its price and Telstra's price did not, in his Honour's view, assist Optus. The false dominant message was conveyed in the first part of the advertisement which contained the guarantee of total bill saving. His Honour took the view that this false dominant message was not ameliorated by the later statement that if you "switch to us and take advantage of the Optus guarantee, you will save".

His Honour also said that the same conclusion could be reached by a different route. The material submitted by Optus acknowledged that it was cognisant of the subtle distinctions involved in the advertising of charges. Optus had left the position blurred.

Similarly, a statement by Optus that it was cheaper to "anywhere at any time" was misleading or deceptive because those subscribers to the Telstra Flexi-Plan might well have international calls cheaper than the equivalent Optus call depending upon the time and other circumstances of the call involved.

The balance of his Honour's judgment relates to question of balance of convenience and the discretion of the court that both being factors involved in whether or not an interim injunction should be granted. However, his Honour was satisfied that Telstra had presented a case that there was a serious issue to be tried and that the balance of convenience favoured the grant of interlocutory relief. His Honour was further satisfied that there were no discretionary reasons for refusing relief. Accordingly, the interlocutory injunction requested by Telstra was granted.

Lessons from the Case

The case is a useful one in collecting relevant authorities on the question of comparative advertising, "half truths" and "impressions". His Honour's research is not limited only to Australian material. The case reinforces the principles that impressions are paramount in television advertising and that there is a special duty cast on advertisers to ensure that comparisons are accurate. If a comparison cannot be truly made or if a comparison is based on assumptions which may not be correct, then comparative advertising should not be engaged in. The case is likely to become a standard citation, because of its research, on the rights and wrongs of television advertising and comparative advertising.

Nationwide News V ACCC

Nationwide News conducted a promotion in newspapers which concerned an offer to readers of a "free" mobile telephone. As a condition of receiving the phone, the purchaser of it was required to enter into a contract which involved a total expenditure of $2,295.00. The ACCC prosecuted Nationwide News. At trial, Nationwide was found to have breached section 53(e) and section 53(g) of the *Trade Practices Act* (covering misleading representations in relation to price and misleading representations in relation to conditions, warranties and guarantees respectively). At trial, Nationwide News was held to have breached these two sections. The present case was an appeal from the trial decision. The leading judgment was written by Lindgren J, Spender J and Lehane J agreeing with his Honour's judgment.

The Decision

The main issue in the case was the interpretation of the word "free". Nationwide News submitted that the words "conditions apply" which appeared in the advertisement qualified the "freeness" aspect of the offer. In fact, those supplied with mobile phones had to enter into an arrangement with Smartcom Telecommunications pursuant to which the phone owner had to pay a connection fee, a delivery charge, a security deposit and an amount of $130.00 a month in advance for a minimum of 15 months. The monthly payment was in respect of access to the Vodafone mobile digital network and included the first $120.00 of calls per month.

His Honour held the following propositions applicable to the word "free":

- The word "free" is rich and diverse in meaning. There is no dictionary definition of the word "free" which can be applied in all cases. Depending on circumstances, the word "free" may mean not subject to a payment or given or provided without charge or payment or gratuitous.

- Advertisers have been charged not infrequently with failing to provide goods or services which are "truly free" as advertised.

- There are many conditional "free" goods offers which result in deception of purchasers. In some cases, the merchant may increase the advertised price of an article over the ordinary and customary selling price in an amount sufficient to offset, in whole or in part, the cost of the "free" goods. In other cases, the merchant may substitute inferior merchandise for that ordinarily and customarily sold at the designated price involved in the transaction thereby recovering in whole or in part the cost of the "free" goods.

- Offers of "free" goods conditional on the purchase of other merchandise may appear at first impression to be unconditional offers of "free" goods. This is brought about by the prominent featuring of the "free" goods offer in a way to obscure or minimise the condition attached. This will result in deception and it is not sufficient that the purchaser be made fully aware of any conditions before the transaction is finally consummated. The purchaser should be fully apprised of all the terms and conditions of the offer at its very inception.

- It is misleading or deceptive to reiterate the concept of "free" items

when these items may be acquired only with some significant loss or outgoing by an offeree who accepts them. In this respect, his Honour noted the decision of Gummow J in *Fraser v NRMA Holdings Limited* (1994) ATPR ¶ 41-346 in which his Honour dealt with the question of what was meant by "free shares".

His Honour said that whilst each case turns on its own facts, it is clear that there is judicial recognition of the propensity of the word "free" in advertising to mislead or deceive. An advertiser relies on common understandings at its peril. Any respect in which goods or services offered as "free" may not be free should be prominently and clearly spelt out so that the magnetism of the word "free" is appropriately qualified.

In his Honour's view, this had not occurred in the present case. In reaching this conclusion, he relied upon the above principles. His Honour further stated that the addition of the words "conditions apply" did not detract from that position. Rather, they indicated that upon satisfying certain conditions, the purchaser would be entitled to become the owner of a mobile telephone service still without his having to outlay money or undertake to do so.

Lessons from the Case

Mr Justice Lindgren's judgment is an interesting one. It draws not only upon Australian Federal Court decisions but draws extensively on United States authorities which clearly were of assistance to him in clarifying an area in Australian law which, to date, has received only limited judicial interpretation. It is clear from his Honour's judgment that the word "free" must be used sparingly and that strict parameters are applicable to it. Advertisers would be wise to heed his Honour's admonitions when planning the advertisement of "free" goods.

Conclusion

In the telecommunications industry, there has been strong competition of recent times and thus a tendency perhaps to obscure the true worth of deals offered to the public. The cases clearly illustrate that the judiciary will not be party to any sliding in standards and advertisers who have an elliptical view of the truth will face considerable litigation risks as a result of their views. In particular caution is required by advertisers in comparative advertising and in advertising "free" items.

Dr Pengilley is the Sparke Helmore Professor of Commercial Law at the University of Newcastle and a Consultant to the Sydney office of Deacons, Graham & James. He was formerly a Commissioner of the Australian Trade Practices Commission.
This article was originally published in the Australian & New Zealand Trade Practices Law Bulletin

Sex, Lies and Other Secrets: the Media and Confidential Information

Jason Macarthur outlines the principles of confidential information and some practical implications for the media in Australia.

Journalists rightly argue that its their role to provoke public debate about matters of general interest. Their lawyers, and other free speech proponents, often go a step further and suggest that the media should be free to fulfil that role by publishing information regardless of whether it concerns the private lives of individuals, illicit boardroom dealings or corrupt governments and officials. There is, after all, no general right of privacy in Australia which is recognised at common law or in the Constitution, nor is one likely to be introduced under the present Government. The law of confidentiality, however, provides a limited right to prevent violations of a person's privacy. It recognises the right to disclose inaccessible or confidential information on strict and limited terms and will enforce the obligations imposed on the confidant. It is the enemy of the investigative journalist.

In applying that law, the courts must seek a balance between the interests of individuals to have their confidential matters kept private with the interests of the public at large to be fully informed about important events. In Australia, unlike the U.S., there is no constitutional guarantee to the press to freely report newsworthy issues, except in relation to certain "government and political" matters. The law of confidentiality, places restrictions on the types of information that may be made public by the media and their sources, and when defences to publication will apply.

When the Obligation Arises

An obligation of confidence arises when information which is secret and not merely trivial is disclosed to a person who is expressly or impliedly required to maintain its secrecy. Generally, a media organisation which acquires information as a result of another's breach of confidence may be restrained from publishing the material once it knows, or should reasonably know, that the material is confidential.

The situation in which information is obtained will often suggest that it is confidential. For example, a journalist who is told in confidence about a company's unlawful activities by one of its employees will be assumed to be aware of the nature of the information and the employee's broken obligation to the employer. Where initial ignorance of the obligation is reasonable in the circumstances, the commencement of proceedings by a plaintiff may amount to notice of the obligation, thereby binding the journalist and restraining subsequent publication.

Special Relationships

A number of relationships are generally recognised at law as giving rise to an obligation of confidence, including doctor and patient, lawyer and client, priest and penitent, husband and wife, and employer and employee. Personal secrets between friends may also be protected in certain circumstances. In the UK case *Stephens v Avery* the defendants included the proprietors of a Sunday newspaper which published a story about a lesbian relationship carried on between the plaintiff and another woman who had been killed by her husband after he had discovered his wife's extra-marital lesbian affair. The Court held that publication of the story may give rise to an action for damages even though there was no recognised relationship of confidence at law between the original parties to the secret.

The media will often resort to the following two main lines of argument in confidentiality cases. The first argumant is generally raised in opposition to the granting of an injunction to prevent publication and the second operated as a defence to an action after publication has already taken place:

1. the information is in the public domain and therefore is no longer secret; and

2. the publication was justified in the circumstances on public interest grounds.

Loss of Confidentiality

Secrets cease to be confidential and can no longer be protected from publication once they become common knowledge or within the public domain. Confidential information will not fall into the public domain if it is disclosed only to a limited audience so that its "relative secrecy" prevails. Unfortunately for the media in particular, there are no clear cut rules or judicial guidelines to safely predict in what circumstances and to what extent information must be disclosed before it enters the public domain. Pragmatism rather than principle dominates the decisions in this area.

In *G v Day* the Truth was restrained from publishing the identify of the plaintiff who had reported a sighting of Frank Nugan to the Corporate Affairs Commission at a time when Mr Nugan had in fact died some months earlier. At the time the injunction was granted the plaintiff's name had already been broadcast on two occasions on Channel 10's Sydney news. However, the court held that because the references were merely "transitory and brief" and formed no permanent public record, the plaintiff's identity remained confidential.

On the other hand, in *Commonwealth -v- John Fairfax & Sons*, an injunction to prevent publication of a book containing foreign and defence policy secrets was refused because, at the time of the application, over 60,000 copies of the Sydney Morning Herald had been published containing an extract from the material. Furthermore, copies of the book had already gone on sale. Justice Mason said:

> *"In other circumstances the circulation of about 100 copies of a book may not be enough to disentitle the possessor of confidential information from protection by injunction, but in this case it is likely that what is in the book will become known to an ever widening group of people here and overseas, including foreign governments".*

In the infamous "*Westpac Letters*" case, sections of the media gained access to confidential advices prepared by Westpac's lawyers regarding the bank's potential liability for mismanagement of foreign exchange loans. After the Sydney Morning Herald and The Age published articles containing extracts from the letters, the bank obtained injunctions restraining further publication in the Sydney Morning Herald, the Australian Financial Review and the Melbourne Age and by the journalist who had written the original article. Similar orders were later made against the ABC and the proprietor of the Canberra Times.

Soon after, South Australian Democrat Ian Gilfillan quoted extensively from the letters in a speech to the South Australia Legislative Council. As a result, the information became recorded in a permanent form in the South Australian *Hansard* which contains official transcripts of parliamentary proceedings. The next day parts of the letters were published in the Canberra Times and in the political newspaper Tribune which went on sale outside the Supreme Court in Sydney.

Sections of the media then applied (unsuccessfully) to have the injunction lifted on the basis that the information had passed into the public domain. Justice Powell, in refusing the application, stated that he wasn't convinced that "the detail - as opposed to the general nature" of the material had become public knowledge. While the entire contents of the letters had not yet been reproduced verbatim, this fails to explain why the sections which had by then been widely disseminated were not themselves considered within the public domain and therefore available to the media at large.

His Honour also contended that material published in *Hansard* was not readily accessible to the public. While that may be true in practice, it defies legal principle. As other commentators have pointed out, patent specifications, for example, are considered to be in the public domain and accessible once published, regardless of the number of people who actually visit the patents office to examine them.

Confidences Surviving or Reviving after Publication

An obligation of confidence may sometimes survive publication against certain defendants or be revived after a period of time has elapsed since the original disclosure. The so-called "springboard doctrine" has been applied to restrain further publication by the person who made the initial disclosure and who has thereby gained some advantage over others, even after the material has passed into the public domain. It may be used, therefore, to justify penalising a particular defendant for its actions.

In the *Spycatcher* case in the U.K., injunctions were placed on the Guardian and the Observer newspapers restraining publication of allegations made by ex-SIS agent Peter Wright against the British government which had been revealed in earlier proceedings in Australia. Meanwhile, Wright's memoirs were published in the US, protected by First Amendment free speech guarantees. Naturally, sales of the book soared following worldwide publicity for the trials, and in time illicit copies began showing up in Britain and elsewhere.

After nearly two years the media injunctions were finally lifted on the basis that there were enough copies of the book in the UK to destroy any remaining secrecy in the material. The seemingly unfortunate Sunday Times, however, was found to have breached the obligation of confidence by publishing extracts from the book two days prior to its publication in the US. More remarkably, the House of Lords found that the "treacherous" Wright was bound by a "lifelong" duty of confidence to the British government, despite the widespread publication of the material. It restrained Wright from ever freely disclosing what was by that time clearly public knowledge in the UK and elsewhere.

In *Schering Chemicals* a UK court restrained the broadcast of a documentary made by former consultants to a pharmaceutical company which focused on a controversy surrounding pregnancy drugs which the company manufactured. Despite the fact that the issue had been exposed in newspaper reports some time earlier, the court held that the defendants were bound by a continuing obligation of confidence based on their former relationship with the company. Furthermore, the information was said to be no longer in the public domain on the basis that the controversy had long since died down and would by then have been remembered by very few people.

Defence of Justification

Liability for breach of confidence may be avoided if the information discloses some form of wrongdoing on the part of the plaintiff and there is a public interest justifying the disclosure. For example, in one early case there was no liability for publication of information provided by a laundry employee about his employer's involvement in a price-fixing scam which involved a statutory offence.

A broader defence has recently been recognised in the UK based solely on the public interest. The *Lion Laboratories* case, for example, involved the widespread publication of documents leaked by an employee of a firm which manufactured breath testing devices used by British police. The court held that publication was permitted on the basis that the public interest in publication outweighed the public interest in confidentiality, regardless of whether any misconduct was revealed. The public interest lay in ensuring that motorists were not wrongfully convicted for drink driving offences due to the use of the faulty devices.

On the other hand, in *X v Y* another UK court held that the public interest in preventing the publication of the name of doctors who continued to practice despite having contracted the HIV/AIDS virus outweighed the public interest in freedom of the press. In particular, the public interest required that the medical records of AIDS patients be kept confidential so that other sufferers would not be reticent in seeking medical assistance through fear of public exposure.

General Rules

Australian courts, however, have consistently failed to recognise the broader public interest defence. Generally, the defendant must still show some form of misconduct by the plaintiff to escape liability for publication. A number of points emerge from the decided cases:

- *different considerations apply where government secrets are involved - in those cases the burden of proof is reversed and it is the government which must establish a public interest in non-disclosure;*

- *a distinction must be drawn between matters that ought to be disclosed in the public interest and those which are merely of interest to the public. The matter must be objectively serious and not simply interesting but unimportant gossip or rumour, however titillating to readers;*

- *for the defence of justification to succeed, the disclosure may have to be to the "proper authorities" only.*

This last requirement is probably the least satisfactory from the media's point of view. In cases of alleged wrongdoing, for example, the only permissible disclosure may be to the police. Similarly, in cases involving medical danger, the "proper authority" may be public health officials rather than the general public.

Judicial Hostility

It may be argued that Australian courts should follow the example of their more liberal English counterparts in weighing the importance of a free press in the context of public interest debates in confidentiality cases. Such moves would, of course, be counter to the popular notion of protecting the individual's limited 'rights' of privacy in a media-intrusive age. It may also require a reversal of the judiciary's distrust of the media which is at times thinly disguised. The comments of Justice Powell in the *Westpac Letters* case about the "self righteous" media are telling:

"In vigorously arguing for the public's "need to know" and in whipping up public opinion on the matter, they tend to create an environment in which confidentiality becomes much harder to maintain, thereby assisting the case against restraint. However, it is hardly surprising if this creates judicial hostility: judges who feel as if they are being backed into a corner.... will only be human if their reaction is a stiffened resolve to show that they cannot be dictated to by the media."

Jason Macarthur is a lawyer with Tress Cocks & Maddox in the Sydney office. The views expressed in this article are those of the author and not necessarily those of the firm.

International Electronic Money Systems and Money Laundering

Brent Fisse and Peter Leonard examine net-smurfing and other emerging regulatory challenges from electronic payment technologies.

Much has been said about the increasingly global social problem of money laundering and the potential ways in which this problem might be minimised. The advent of electronic payment technologies (**"EPT"**) raises several important questions of regulatory approach and design which have tended to fall between the cracks in the current debate, including the following:

- *EPT are diverse and, although* electronic in operation, are likely to be much more difficult to bring within a common centralised financial transaction reporting system than the relatively homogeneous and concentrated banking system which has been the focus of Australia's significant financial transaction and international wire transfer reporting scheme to date. The trend is towards automating suspect transaction reporting. The rise of EPT service providers raises the question of what can be done to spur the development of such smart systems generally.

- Structured transactions (**"smurfing"**) are a pandemic way of evading the significant financial transaction and international wire transfer reporting obligations under the Financial Transaction Reports Act 1988 (Cth) (**"Act"**) but the present regulatory controls under s 31 of that Act are vague and unworkable. The use of structured transactions will be facilitated by EPT, as in the context of Internet-based smurfing transactions (**"net-smurfing"**) where transaction costs are low and the opportunities for automating structured transactions are high. What practical solutions, if any, are there to this intractable problem?

- AUSTRAC has successfully persuaded at least the major banks to co-operate extensively in gathering and supplying significant financial transaction and international wire transfer information in a format readily usable by AUSTRAC's computer-based screening systems. Is it plausible to suppose that the same "softly, softly" approach will work with EPT operators at least some of whom will be aggressive new entrants with little or no loyalty to the traditions of mainstream Australian retail banking? If not, consideration needs to be given to other regulatory strategies including a statutory "pyramid of enforcement" capable of dealing effectively with non-compliant as well as compliant entities and their staff.

- Developing effective technologies for reporting or searching for relevant intelligence conveyed by means of EPT is likely to impose significant capital and recurrent costs on those who do have to install and operate the systems necessary for reporting and/or searching.

Suspect Transaction Reporting

EPT are diverse and, although electronic in operation, are likely to be much more difficult to bring within a common centralised financial transaction reporting system than the relatively homogeneous and concentrated banking system which has been the focus of Australia's significant financial transaction and international wire transfer reporting scheme to date. The trend is towards automating suspect transaction reporting. The rise of EPT service providers raises the question of what can be done to spur the development of such smart systems by banks and EFT service providers.

There is much disenchantment with suspect transaction reporting regimes, for several reasons. First, it is difficult to distinguish between objectively suspect transactions and those which, short of the threshold, are merely suspected. Secondly, the suspect transaction test is

narrower than that of "unusual" transactions and may easily exclude useful intelligence. Unusual transactions may provide critical investigative linkages, which partly explains why FATF Recommendation 15 envisages that financial institutions will keep a watch out for "unusual" patterns of transactions.

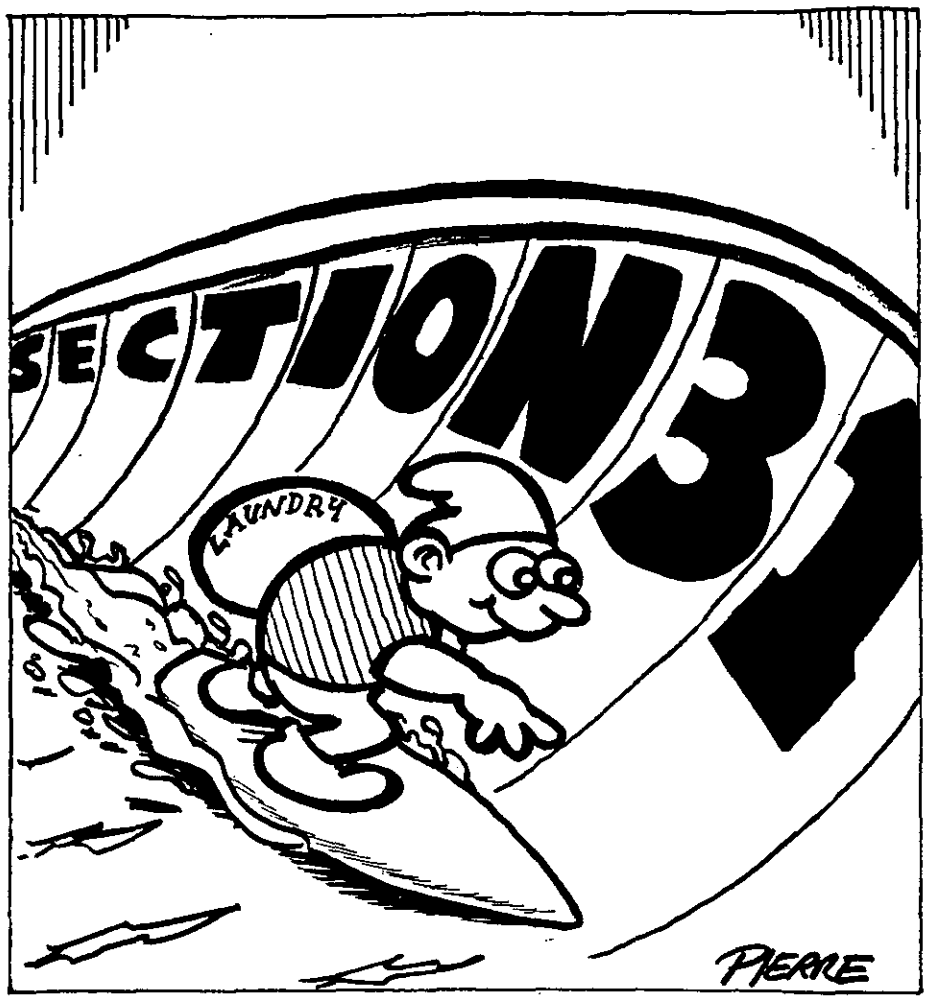
Thirdly, an empirical study by Michael Levi of suspect transaction reporting in the UK[1] indicated a very low strike-rate - around one *arrest* of a suspected drug trafficker per 200 suspect transaction reports. Fourthly, the sheer number of transactions handled by most financial institutions means that any checking of particular transactions is likely to be cursory and quite possibly unreliable.

More fundamentally, suspect transaction reporting based on human suspicion is increasingly outmoded in a world where there are very large numbers of routine electronic banking transactions.

The whole idea of a suspicion-based system is old-fashioned, since unlike burglaries and robberies, most cross-border transactions are conducted purely electronically, without anyone physically seeing them: because of the legislation (and sometimes to guarantee that the transaction will be paid for) customers must be identified, but how are bankers to know whether there is a legitimate "business case" for the myriad of transactions they undertake, and why should it be their business to "shadow" their customers? Legislation does not require them to do those things, but they (and the "informal banking" sector) would have to do so if they were to smoke out all the laundering and fraud.[2]

The more automated the banking and financial system becomes, the less face-to-face contact between clients and employees and the greater the holes in the detection net unless client information is electronically scanned for abnormal patterns and connections. This growing reality has already been recognised in Australia in the context of significant cash transactions reports and details of all wire transfers - the data is automatically sent by the banks to AUSTRAC for checking and the checking process involves a variety of pattern matching and other computer-based detection routines.[3]

AUSTRAC has moved towards relying more on suspect transaction reporting based on the automated collection of objective data rather than reliance on the subjective human judgment of tellers and



their supervisors. Shortly it is planned that computerised programs within banks may generate Suspect Transaction Reports, at least in relation to certain rudimentary indicators of possible money laundering. This project (called autoSUSR) will help to deal with some of the criticisms by law enforcement agencies that certain rudimentary behaviour is not reported.[4]

Given this trend towards automated suspect transaction reporting, the growth of EPT service providers may well impel further development of smart systems.

One approach would be to fast track the development of smart reporting systems technology for EPT service providers and other financial institutions by AUSTRAC and to amend s 17 of the Act so as to give EPT service providers and other financial institutions the right to opt out of the standard suspect transaction reporting requirements where they enter into an enforceable undertaking with AUSTRAC to develop and install a smart system compatible with AUSTRAC reporting protocols and which alone or in combination with human oversight procedures is approved by AUSTRAC as a system reasonably capable of achieving the reporting of unusual transactions.

This is an adaptation of the enforced self-regulation approach advanced by John Braithwaite in the context of suspect transaction reporting by banks. The model of enforced self-regulation envisaged by Braithwaite would require financial institutions to spell out the particular way in which they would go about detecting suspect transactions and ensuring that staff acted according to that plan.[5]

Whether or not there are sufficient incentives for EPT service providers to take the enforced self-regulation route is another question. A "softly, softly" approach may be seem insufficient (see section 4 below). Another key issue is who is to pay for the costs of developing smart systems.

The Problems with Smurfing Offences Under Section 31

The recent decision of the high Court in *Leask v the Commonwealth*[6] that s 31 of the Act is within consitutional power does not address the concerns raised at the outset of this article about the evasion of

reporting obligations under the Act by means of structures transactions.

Internal controls by financial institutions against structured transactions work on the basis of checks for cash deposits by a customer which in aggregate exceed the threshold amount at which a single cash transaction must be reported. One major difficulty is to indicate to financial institutions the time-frame within which they are obliged to aggregate deposits without also letting smurfs know what adjustments they need to make to avoid getting caught by the aggregation tests. As explained below, this problem arises under the anti-smurfing provisions under the Act.

The smurfing offences under s 31 of the Act are defined essentially in terms of the test whether, given the nature of the transactions, it is "reasonable to conclude" that a dominant purpose of the transactions was to evade the reporting obligations under the Act. The test under s 31 is not related to any given period during which financial institutions are expected to aggregate transactions involving a particular customer. There is no specific obligation under the Act to aggregate deposits or other cash transactions. Instead, "the aggregated value of transactions" is one of the indicia (see s 31(1)(b)(I)(B)) which the trier of fact is to consider when applying the "reasonable to conclude" test.

The *ex post facto* nature of the test of liability under s 31 puts banks and other financial institutions in a precarious or impossible position. The "reasonable to conclude" test implies that financial institutions are under an obligation to aggregate cash transactions yet they are not in a position to know what exactly that obligation requires of them at the time when the transactions take place. Worse, the test is not applied until the matter is determined by the trier of fact. Financial institutions thus remain under an obligation to aggregate deposits until such time as the matter is decided in a prosecution or civil proceeding. So open-ended an obligation to aggregate is not merely vaguely defined but impractical. To comply with it, conceivably a bank would need to aggregate deposits on a perpetually rolling basis, perhaps for years after an initial transaction took place. If the legislation does not require banks to go to such extreme lengths, where is the line to be drawn?

It is also unclear whether the required standard of compliance is the same across the wide variety of organizations and bodies subject to s 31, or whether it varies depending on the technology available to the particular organization. What exactly are banks and other financial service providers supposed to do to keep track of deposits or other transactions at their various branches? A major interstate or international bank may have a sophisticated computer network which makes the task of aggregation a relatively simple one, whereas a small finance company or on-line service provider may lack any corresponding facility.

If, for example, a bank has a computer-based tracking capability that enables it instantaneously to aggregate all deposits made at any branch within, say a 24-hour period, then it may well be "reasonable to conclude" on the basis of the information available to that bank that the sole or dominant purpose of the customer was to evade the reporting requirements. On the other hand, if a bank does not have such a computer-based capacity, perhaps it is unreasonable to arrive at the same conclusion.

Section 31 does not resolve the most critical question here, which is whether or not banks and EPT service providers are expected to install systems that will enable aggregation of deposits made at all branches or for all machines dispensing smart cards, instantaneously or within say a daily or other period. Many financial institutions in Australia as elsewhere do not presently have the capacity to aggregate deposits at all branches even on a daily basis. If they are expected to acquire some greater capacity, it seems harsh to make them run the gauntlet of an ill-defined penal provision. Moreover, installing adequate systems takes time and systems cannot sensibly be installed until it is known what exactly the expected standards of aggregation are. The same applies to the emerging EPT industry and the planning that needs to go into their hardware and software requirements.

Possible Solutions

One possible solution would be a system, developed in conjunction with the banking and finance and EPT industries, under which different aggregation periods are used by different financial institutions at different periods arranged on a secret roster basis.[7] Financial institutions would then know exactly where they stand, yet smurfs would not be presented with aggregation rules which could easily be circumvented. Such a system supposes that banks and other financial institutions have the technical capability to alter the time settings of their aggregation programs periodically at low cost. It also assumes that the roster arrangements could in fact be kept secret from the smurfing underworld.

Another possible approach is via enforced self-regulation, with each bank or EPT service provider determining its own aggregation rules - smurfs would not be faced with a standard aggregation period which could easily be circumvented but with many unknown and different aggregation periods[8]. This approach assumes that the aggregation period selected by a given bank could in fact be kept secret from smurfs. It does not necessarily assume a technological capacity to change the aggregation periods periodically at low cost. However, such a capacity might well be essential to reduce the risk of disclosure.

The only approach which seems to be capable of avoiding the otherwise high risk of the aggregation periods being leaked to smurfs is a centrally controlled system under which aggregation periods for each and every financial institution are selected randomly by a computer program and then transmitted and deployed in such a way that no human agent has access to the random sequence. Utopian?

A further hurdle to aggregation is the possibility that transactions could be structured across a number of institutions (i.e. using digital cash from a number of different issuers) as well as by breaking the total value of such transactions into smaller sums.[9] Inter-bank aggregation of transactions would present substantial practical difficulties, in addition to further privacy issues.

"Softly, Softly" Regulation, or Negotiation and Settlement Within a Statutory Pyramid of Enforcement?

A luminous feature of AUSTRAC's record is its success in persuading at least the major banks to co-operate extensively in gathering and supplying significant financial transaction and international wire transfer information in a format readily usable by AUSTRAC's computer-based screening systems.

Whether the same spirit of co-operation is likely to be attainable in the context of EPT service providers is another question. At least some will be new entrants committed to developing their

businesses at low cost may balk at incurring the expenditure which may be needed to introduce significant transaction and international funds transfer funds reporting systems which are compatible with AUSTRAC's data handling systems. Not all will agree with the merits of being subjected to the reporting obligations imposed under the Act or the wisdom of voluntary co-operation for the sake of community interest.

Consistently with the objective of achieving co-operation and consensus as far as possible, and assuming that EPT service providers are or will be regulated under the Act, consideration needs to be given to strengthening the Act so as to enable AUSTRAC and other enforcement agencies to help bring any non-compliant EPT service providers and other "new wave" financial institutions into line.

AUSTRAC has indicated its wish to have additional civil remedies to strengthen its hand.[10] The design of any such amendments is best approached from the broader perspective of a "pyramid of enforcement" strategy capable of dealing with non-compliance with remedies and sanctions of whatever severity and type required to bring about compliance and mutual co-operation.[11] Such a strategy, which would require some amendments to the Act is already a well-known feature of ACCC enforcement policy and practice (it is less apparent on the part of the ASC, which has been criticised to some extent for failing to adopt a sufficiently explicit policy for the settlement of enforcement actions).

Who will Bear the Enforcement-related Cost of new EPT Reporting and/or Searching Requirements?

Developing effective technologies for reporting or searching for relevant intelligence conveyed by means of EPT is likely to impose significant capital and recurrent costs on those who do have to install and operate the systems necessary for reporting and/or searching. Australian banks, like their US counterparts, have generally taken the costs on the chin in the past, but this seems largely a quirk of history. It is significant that carriers successfully objected to the "enforcement agency user does not pay" principle which surfaced under the draft 1997 telecommunications legislation in the context of interception under the *Telecommunications (Interception) Act* (Cth) but which was later abandoned in the *Telecommunications Act* 1997 (see s 314). EPT service providers should be quick to make the same point if attempts are made to enlist them as unpaid deputies to fight money laundering.

It is far from obvious why the social cost of providing interception capability or monitoring capability should be imposed on financial institutions rather than spread more through general taxes as in relation to the costs of improving stolen vehicle tracking systems or enhancing surveillance technology for detecting terrorists or plane hijackers. EPT service providers and other financial institutions should hold out for the user pays principle and rely on the model provided by s 314 of the *Telecommunications Act*.

Conclusion – Balance or Bust?

Michael Levi has observed of regulatory controls against money laundering that:

> *"[t]he trick of regulation is to minimise the illegitimate exploitation without wrecking the economic dynamism"*[12]

The regulatory challenges canvassed in this paper intensify rather than reduce what is already a difficult balance.

1 Levi, *"The Reporting of Suspicious Money-Laundering Transactions"* (1994))

2 Michael Levi, "Money Laundering and Regulatory Policies" in "Savona" ed. *"Responding to Money Laundering: International Perspectives"* Amsterdam: Harwood Academic, 1997 at 279.

3 See AUSTRAC, *AUSTRAC Papers 1992.*

4 AUSTRAC, *The Next Phase* (1995) 14.

5 Braithwaite, *"Following the Money Trail to What Destination?"* (1993) 44 Alabama Law Review 657, 665.

6 Unreported, 1996.

7 Fisse, Fraser and Coss, eds, *The Money Trail*, Sydney: Law Book Co., 1992 at 186.

8 Braithwaite, *"Following the Money Trail to What Destination?"* op cit. at [ ]

9 Tyree *Digital Cash* Sydney: Butterworths, 1997 at 4.89.

10 AUSTRAC, *The Next Phase* (1995) 22-23.

11 See further Ayres and Braithwaite, *"Responsive Regulation"* New York: Oxford University Press, 1993.

12 Levi, *"Money Laundering and Regulatory Policies"* op cit. at 260.

Brent Fisse and Peter Leonard are partners with Gilbert and Tobin.

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

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:

Andrew Lambert
c/- Deacons Graham & James
Gold Fields House
Circular Quay
SYDNEY NSW 2000
Tel: +61 2 9330 8000
Fax: +61 2 9330 8111
Email:
andrew.lambert@dgj.com.au

OR

Jason Macarthur
c/- Tress Cocks & Maddox
Level 20, 135 King Street
SYDNEY NSW 2000
Tel: +612 9228 9276
Fax: +612 9221 4988
Email:
jecm@tcm.com.au

Communications and Media Law Association

The Communications and Media Law Association (**CAMLA**) was formed in 1976 and 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
- contempt
- broadcasting
- privacy
- copyright
- censorship
- advertising
- film law
- confidentiality
- telecommunications
- freedom of information
- 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, Attorney Generals and members of government bodies such as the Australian Broadcasting Authority, the Australian Competition & Consumer Commission, the Australian Communications Commission, the Film Censorship Board, the Australian Film Commission 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.

To: **The Secretary, CAMLA, Box 545, Glebe, NSW 2037**
Tel/Fax: +61 2 9960 1645

Name: .....

Address: .....

Telephone: ..... Fax: ..... DX: .....

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 $95.00
- Corporate membership $425.00
  (list names of individuals, maximum of 5)
- Student membership $35.00
- Subscription without membership $95.00
  (library subscribers may obtain extra copies for $10.00 each)

Signature .....