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

Contributions and Comments

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

Contributions in hard copy and on disk and comments should be forwarded to:

Shane Barber
c/- Truman Hoyle Lawyers
Level 18, ANZ Building
68 Pitt Street
SYDNEY NSW 2000
Tel: +612 9232 5588
Fax: +612 9221 8023
email:
sbarber@trumanhoyle.com.au

or

Page Henty
c/- Allens Arthur Robinson
The Chifley Tower,
2 Chifley Square,
Sydney NSW 2000
Tel: +612 9230 4000
Fax: +612 9230 5333
email: Page.Henty@aar.com.au

Communications and Media Law Association

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

Issues of interest to CAMLA members include:

- defamation
- contempt
- broadcasting
- privacy
- copyright
- censorship
- advertising
- film law
- information technology
- 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, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

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

CAMLA Website

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

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

Name: .....

Address: .....

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

Principal areas of interest: .....

.....

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

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

Signature .....

Communications LAW B•U•L•L•E•T•I•N

THE OFFICIAL PUBLICATION OF THE COMMUNICATIONS AND MEDIA LAW ASSOCIATION INCORPORATED

Print Post Approved PP: 234093/00011 EDITED BY SHANE BARBER AND PAGE HENTY Vol 23 No 4 2004

Separating Telstra: Legal Issues Surrounding the Divestment of Foxtel and the HFC Cable Network

Daniel Yap, in this CAMLA Essay Prize winning entry, examines the legal issues that arise from the ACCC's recommendation that Telstra divests its hybrid fibre coaxial (HFC) network and 50 per cent ownership of Foxtel to encourage competition across the pay tv, telephony and broadband sectors.

In June 2003, the Australian Competition and Consumer Commission (**ACCC**) released a report on the wider competition effects of emerging structures in the pay tv market.[1] The report recommended Telstra divest its hybrid fibre coaxial (**HFC**) network and 50 per cent ownership of Foxtel to encourage competition across the pay tv, telephony and broadband sectors. At the time, the Federal Government rejected this recommendation, arguing that the costs of the divestiture outweighed the perceived benefits.[2] In contrast, the Australian Labor Party strongly endorsed the ACCC recommendations. Although the recent Coalition victory greatly diminishes the prospect of Telstra being forced to divest its HFC cable and Foxtel shareholding, this paper provides an analysis of the regulatory issues the government faces in the event of such a scheme.

BACKGROUND

Telstra is the dominant telecommunications player in Australia and one of the most vertically and horizontally integrated operators in the world[3]. It owns both the public switched telecommunications network (**PSTN**) and the largest HRC cable network in Australia. The PSTN is a ubiquitous network, reaching almost every Australian home[4] and is primarily used for fixed line telephony. The Telstra HFC network was built as a defensive ploy to duplicate the area covered by its competitor, Optus, and passes through 2.5 million homes. Telstra currently offers pay tv and broadband services over its HFC network while Optus also offers voice telephony on its cable.

Telstra owns 50 per cent of Foxtel, the pre-eminent pay tv operator in Australia, with approximately 880,000 retail subscribers and 200,000 wholesale subscribers[5]. The dominance of Foxtel in the pay tv market and Telstra's dominance in the telecommunications market serves to reinforce each other[6]. Telstra has the incentive to restrict the supply of content and access to the HFC network from those competing with its supply of telecommunications. Moreover, Telstra has refrained from introducing services on the PSTN network that would cannibalise revenues from the HFC network[7].

In order to address these concerns, the ACCC recommended the separation of the pay tv business and HFC cable. The divestitures would increase Telstra's and Foxtel's willingness to supply

INSIDE THIS ISSUE

CONTENTS

content and carriage services and thereby encourage competition and the development of new technology platforms for consumer benefit.

DIVESTITURE POWERS OF THE GOVERNMENT

Although the Federal Government owns 50.1 per cent of Telstra, the power to manage the business and affairs of the company is vested in the board of directors[8]. Telstra directors are unlikely to instigate the ACCC recommendations without government intervention[9]. Telstra has made significant investments in both assets, recently upgrading the HFC network to provide digital tv and Foxtel is yet to break even[10]. The pay tv provider is a key defensive and a strategic investment for the future. Foxtel allows Telstra to bundle services to reduce customer loss, while providing access to premium content should internet data services become commonplace.

The government may be able to force a sale through the obligations imposed by the *Telstra Corporations Act 1991*,[11] which limits the power of Telstra directors[12].Under section 9, the Minister could give written directions to Telstra to dispose of its shareholding in Foxtel and the HFC cable because it is necessary in the "public interest"[13].

However, it is uncertain whether the scope of the power can extend to such a drastic action as no directions have been issued under section 9 to date[14]. A greater concern is whether the divestitures would be in the best interests of shareholders. Although Telstra directors would be acting under the Ministerial direction, they would still appear to be subject to statutory and general law duties[15]. It would be difficult for directors to discharge these duties unless a scheme delivered fair compensation for Telstra shareholders.

The sale of the HFC cable would be a huge loss for Telstra because it has made a significant investment in the network with an estimated cost value of $3 to $4 billion[16]. Telstra's ability to extract synergies from its investment in the network and Foxtel through bundling suggests it is not economically viable for a stand alone pay tv service provider to purchase the infrastructure at its value to Telstra. Potential buyers of the businesses are unlikely to pay the cost value[17] which would be close to a fair level of compensation.

The Government is advised to obtain an independent expert's report to establish a reasonable value for the assets. The report would probably find a shortfall between the value of the assets to Telstra and the bidder's purchase price. There is a strong likelihood government would have to make up the difference and pay Telstra compensation to avoid shareholder litigation.

SALES OBSTACLES

Although the government may have power to force a sale of Telstra's assets, the divestitures could be blocked by other parts of the current regulatory regime. This section examines ownership structures where such regulatory issues may arise.

Sale of HFC Infrastructure to Foxtel

Foxtel is the only party capable of extracting synergies to pay the highest price for the network. However, the purchase is probably not even technically viable for Foxtel because it can operate at a much lower cost by renting the capacity from Telstra and/or Optus cable.[18]

The ACCC has power under section 50 of the *Trade Practices Act 1974 (Cth)* (**TPA**)[19] to prevent acquisitions that would have the effect, or likely effect, of substantially lessening competition.[20] While the sale of the HFC network will encourage infrastructure competition[21], the divestment to Foxtel will only entrench its position as the pre-eminent pay tv service provider in Australia. Foxtel's direct control of both carriage and content introduces incentives for the company to restrict access to the HFC cable and its pay tv channels from other networks. This situation can be distinguished from Optus' ownership of

Victorian Court Action Over Alleged Unfair Terms In Mobile Phone Contracts

Bridget Edghill reviews the action taken by the Victorian Government in relation to alleged unfair terms in mobile phone contracts.

The Victorian Bracks Government has launched proceedings against Telecom Corp of New Zealand's (**NZT**) Australian telecommunications subsidiary, AAPT. The court action seeks to force AAPT to remove a number of terms from their mobile phone contracts which it considers to be unfair in light of the *Fair Trading Act 1999 (Vic)* (**Act**).

The proceedings in the Victorian Civil and Administrative Tribunal (**VCAT**) allege that certain terms of the AAPT contract contravene the Unfair Terms in Consumer Contracts provisions contained in Part 2B of the Act. Pursuant the Act, a contract term is considered unfair,

> *"if contrary to the requirements of good faith and in all the circumstances, it causes a significant imbalance in the parties' rights and obligations arising under the contract to the detriment of the consumer."*

The Victorian Consumer Affairs Minister, John Lenders observed that *"there are 11 clauses within AAPT's mobile phone contract and seven terms in their prepaid phone contracts that we allege are unfair and therefore void."*1

COMMON TERMS DEEMED TO BE UNFAIR

The legal action arose after Consumer Affairs Victoria wrote to Telstra, Optus, AAPT, '3', Orange, Virgin and SIM PLUS in August 2004, urging them to co-operate with Consumer Affairs Victoria to modify their consumer contracts to comply with the Act.

In particular, the Victorian Government identified a number of common terms in mobile phone contracts that it considers to be unfairly biased towards suppliers2:

- *Lock-in-terms (unilateral change terms)* that allow the supplier to vary important terms of the contract, or to perform it in a different way to that agreed or expected by the consumer. These terms enable the supplier to make these changes without providing fair and reasonable adjustments, or without the consumer being allowed to terminate the contract without penalty.
- *Punitive dispute resolution terms* that prevent or restrict the consumer's options regarding dispute resolution, with the effect of putting pressure on the consumer to give up, or settle on terms favourable to the supplier.
- *Restriction of reliability* that avoid, limit or restrict the liability of the supplier, its servants or agents for breach of the contract.
- *Penalty clauses* that unfairly inhibit consumers from exercising their rights.

Each supplier, with the exception of AAPT, agreed to work with Consumer Affairs Victoria to review and discuss their mobile phone contract terms. In light of AAPT's apparent unwillingness to cooperate, Victoria's Director of Consumer Affairs, David Cousins, commenced the proceedings which allege that certain term in AAPT's standard telephone and pre-paid mobile phone contracts contravene the Act as the terms allow AAPT to unilaterally change the contract and suspend services without notice, later charging a reconnection fee.

IMPACT OF DECLARING TERMS 'UNFAIR'

Pursuant to section 32Y of the Act, if Consumer Affairs Victoria is successful in having the terms declared to be unfair, the unfair terms will be void.

With more than 14 million mobile phones in Australia3, terms similar to those identified as being unfair by the Victorian Government are commonplace in phone contracts. A ruling in favour of AAPT will undoubtedly lead to other suppliers reviewing their own contracts.

The other telephone service providers were given until the end of 2004 to review there consumer contracts and notify the Victorian Government as to their actions and progress in modifying their own contracts to ensure that they comply with the Act. Service providers that fail or refuse to do so may risk being included in the action against AAPT.

Bridget Edghill is a lawyer with Sydney corporate and communications law firm, Truman Hoyle.

1 AAP, "Vic Govt launches action against AAPT", 15 December 2004, The Age

2 Media Release from the Minister for Consumer Affairs, "Bracks Government Puts Mobile Phone Companies on Notice to Comply with Victorian Fair Trading Law", 8 August 2004, available at http://www.consumer.vic.gov.au/cbav/fairsite.nsf/pages/of_media_releases_080804?Open

3 "Vic Govt goes after mobile phone companies with new fair trading law" 10 August 2004, available at http://www.wps.com.au/news.html?newskey=476.

FISA Court from any liability to any other person for such production.

A further cause for concern is that the *US Patriot Act* eliminates the barrier between national security surveillance and US local law enforcement. The fear is not just that personal information may be disclosed to US law enforcement agencies in the course of anti-terrorism investigations, but that the information obtained may be used by US authorities to bring criminal charges against people for all manner of offences. A decision by the highly secretive Foreign Surveillance Review Court confirmed that the FBI now has much more latitude to share information obtained through national security surveillance with local US criminal law enforcement agencies13.

WHAT CAN BE DONE?

Privacy advocates have recommended new legislation to make it an offence to disclose information under the circumstances envisaged in the *FISA*, supported by sanctions against the individuals concerned. In the current climate, this does not appear to be likely, especially in Australia where the federal government has unreservedly supported the US government's anti-terrorism laws and 'war on terror' generally, and has strengthened our own laws accordingly.

Australian organisations concerned with the security of the personal information which they acquire may need to follow the example of the South Australian and British Columbian governments in reviewing their outsourcing arrangements and policies. One answer would be to cease outsourcing IT operations to companies subject to the jurisdiction of the *FISA*, or simply to cease outsourcing at all. In any proposed outsourcing agreement between a holder of personal information and a company subject to *FISA* jurisdiction, it may be prudent to consider including an express prohibition on disclosures under foreign laws such as *FISA*, except where expressly required or permitted by Australian court order, and the contractual remedies for such disclosure, regardless of whether made in accordance with the laws of the foreign country. Of course, detecting a breach, and enforcing a remedy, remains problematic in light of section 1861(d).

David Chan is the General Manager of Argo Lawyers in Sydney and has worked in the IT and legal industries for over 10 years.

1 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)

2 For an extensive review of FISA, see Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* (CRS Report for Congress, 2003); the report is available on the website of the Federation of American Scientists: www.fas.org.

3 Stephen J. Schulhofer, "No Checks, No Balances: Discarding Bedrock Constitutional Principles" in Richard C. Leone and Greg Anrig Jr., eds., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (New York: Public Affairs, 2003) 74 at 81.

4 www.gartner.com

5 Hayes, Simon, "US law raises privacy worries", *The Australian* (2 November 2004)

6 Ibid.

7 British Columbia. Office of the Information and Privacy Commissioner. Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing.

8 1988 (Cth)

9 Schedule 3 *Privacy Act 1998 (Cth)*

10 US Privacy Act 1974

11 Supra Note 5

12 Ibid.

13 *In Re Sealed Case* 310 F.3d717 (Foreign Intelligence Surv. Ct. Rev 2002)

a HFC network and pay tv service because of Foxtel's stronger market position and its direct control over content (Optus uses Foxtel content). Therefore, the ACCC is unlikely to allow the divestment of the HFC cable to Foxtel.

The benefits of divesting the HFC cable are reduced if Telstra sells the Foxtel shareholding. Although Telstra's continued ownership of the PSTN and HFC networks reduces opportunities for infrastructure competition between these two networks, it encourages other forms of competition. The willingness of Telstra and Foxtel to supply key inputs to competitors will increase and Telstra's bundling ability and market power will be diminished. Importantly, the divestiture of Foxtel will remove incentives for Telstra to discourage other pay tv operators from accessing the HFC network and prevent Telstra from restricting access to Foxtel content to other operators.

The economic and legal analyses suggest that ownership of the HFC network should remain with Telstra.

Sale of Telstra's shareholding in Foxtel - News Ltd and/or PBL

News Ltd and PBL are the most likely bidders for Telstra's 50 per cent shareholding in Foxtel because they each own a 25 per cent stake and have first right of refusal over Telstra's holding[22]. Both companies have contributed significantly towards the $8 billion invested in the subscription television industry since 1995[23] and will be keen to see some return from Foxtel, which is yet to reach profitability. News Ltd and PBL are in the best position to offer the highest price because their control of pay tv content provides them with leverage to extract synergies from Foxtel, unlike other media players.

The Foxtel sale will also be assessed under the anti-competitive provisions in the TPA. The removal of Telstra increases the concentration of media ownership in Australia[24]. Cross media ownership laws regard subscription tv as a separate arena from the traditional print, commercial radio, broadcasting and commercial television markets and place no restrictions on the ownership of a pay tv service[25]. Nevertheless, section 50 of the TPA may prevent an increased shareholding in Foxtel by News Ltd or PBL.

One option is the purchase of Telstra's shareholding in Foxtel by PBL. PBL's ownership of the Nine Network and Foxtel would give it control over the dominant free-to-air network and pay tv provider. The ACCC notes that the joint ownership gives Foxtel the incentive to discriminate in favour of the Nine Network when retransmitting FTA channels on the pay tv platform. Moreover, PBL would have the ability to jointly purchase FTA and pay tv rights, to the exclusion of other FTA providers. PBL will also have strong incentives to restrict other pay tv providers from gaining access to Foxtel content because of its interest in Fox sports.

Another option is the purchase of Telstra's shareholding jointly by News Ltd and PBL or by News Ltd alone. PBL's influence would be reduced and any significant discriminatory treatment favouring retransmission to the Nine Network would have to be acceptable to News Ltd[26]. In this situation, there are less cogent reasons for the ACCC to block increased control by News Ltd. Nevertheless, the motivation for Foxtel to restrict access to pay tv content (produced by News Ltd) from other providers exists.

There could be an impediment against the sale of Telstra's holding to News Ltd or another foreign company imposed by the *Broadcasting Services Act 1992* (**BSA**)[27]. News Ltd is planning to reincorporate in the U.S although it will retain a secondary Australian listing[28]. Under section 109 of the BSA, a foreign person is not permitted to have company interests of more than 20 per cent in a subscription television broadcasting license[29]. News Ltd would become a foreign person under the BSA. Since the primary listing of News Ltd will be in the U.S, natural persons who are not Australian citizens will hold interests in the company

exceeding 50 per cent. Nonetheless it could be possible for News Ltd to circumvent the BSA restrictions on foreign ownership by creative corporate structuring[30]. Otherwise the government could also consider amendments to the BSA to permit News Ltd's holding.

Foreign acquisitions can also be prohibited by the Treasurer under the *Foreign Acquisitions and Takeovers Act 1975 (Cth)*[31], if deemed contrary to "national interest"[32]. However, as a matter of practice, the ownership restrictions in the BSA are regarded as conclusive, and foreign acquisitions that contravene these limits are treated by the Treasurer as contrary to national interest[33].

The preceding discussion confirms it is "legally and technically tricky" [34] to force a sale of Telstra's Foxtel investment. While a sale to either PBL or News Ltd will achieve the highest price and reduce the need for government compensation, it could be blocked by the ACCC for substantially lessening competition. On the other hand, the sale of the Foxtel to a party not involved in pay tv content or carriage, or a public listing of Foxtel would ameliorate anti-competitive concerns. However under both situations, the price paid by another party or individual investors is unlikely to match the offers of PBL or News Ltd, leaving the government with the prospect of paying Telstra investors significant compensation.

The economic analysis suggests that Foxtel should be sold to News Ltd and/or PBL. The global pay tv industry has suffered financially and is yet to reach profitability. The high costs of content[35] suggest it is not viable for an independent operator to purchase Foxtel without access to content. On the other hand, the legal analysis indicates that an ownership structure involving News Ltd or PBL has the strong potential to substantially lessen competition. However, the current regulatory regime or changes to the regime can reduce these concerns and could encourage the ACCC to approve the transaction.

REGULATORY ISSUES AFTER DIVESTMENT

The full separation of Foxtel from content providers, News Ltd and PBL and platforms such as the HFC network reduce the need for government regulation. However, as this separation is unlikely, we assess whether the current regulatory framework encourages competition under the most likely ownership structure.

Access to carriage

Ownership of the HFC cable is expected to remain with Telstra and the sale of Foxtel will increase Telstra's willingness to allow access to the network. However, Foxtel can limit use of the infrastructure because it controls key access points including the set-top units (**STUs**) and service information[36]. The significant sunk costs in establishing the carriage supply chain means that pay tv service providers must go through the Foxtel access points.

Access regulation of the telecommunications industry is set out in Part XIC of the TPA. Under Part XIC, there is a basic right of access to "declared services" where the terms and conditions of access are determined by commercial negotiation or arbitration by the ACCC. Subscription tv is a service declared to be within the scope of Part XIC[37].

Part XIC offers content providers the opportunity to use the HFC network and Foxtel's access points. In December 2003, Foxtel was able to unilaterally set an access and pricing regime for the digital platform, which the ACCC approved[38]. Nonetheless, the terms of regime were a prohibitive factor against actual access[39]. At the time, even large operators such as Channel 7 and 10 stated that they would not proceed with applications to broadcast channels on the HFC network because of costs. However, in a recent decision, the Australian Competition Tribunal ruled that the third parties could challenge for terms better than the approved undertaking[40].

The overturning of the initial ACCC approval indicates the undertaking process is not perfect. Although Part XIC is geared towards commercially negotiated outcomes[41] the access undertaking allows the declared service provider to circumvent negotiations and unilaterally set prices. While the undertaking requires ACCC approval, it has no power to vary the undertaking[42]. One possible area of reform would be to give the ACCC power to negotiate with the access provider, after taking into account industry submissions. This reduces the possibility that undertakings will be anti competitive and restricting rather than promoting access.

Access to content

In 2002, the ACCC accepted section 87B undertakings[43] from Austar, Foxtel and Optus in relation to pay tv content. The subscription tv operators provided a framework including undertakings whereby Foxtel and Optus would not acquire premium movie channels exclusively and where Foxtel and Austar would supply infrastructure operators with their pay tv packages in their entirety upon requested. We suggest that the current access undertakings are sufficient to encourage competition should PBL and/or News Ltd increase their ownership in Foxtel.

Since the initial undertakings, the ACCC has recommended introducing a regime which provides access to individual premium sports and movie content, backed by legislative power. However, this regime would place Optus at a significant disadvantage to other parties because its contractual content sharing agreement (**CSA**) with Foxtel prevents it from "cherry picking" individual popular channels[44]. The structural separation of Foxtel and Telstra reduces the cogency of the ACCC recommendations. In the situation of Foxtel choosing to broadcast over the Optus HFC network, Telstra would be able to apply the access undertakings and supply the Foxtel package on its HFC network.

Although content providers owned by PBL/News Ltd have an incentive to restrict the supply of their channels from Foxtel competitors, the

overly restricted by the sole purpose test. Between 1979 and 2001, the FISA Court approved all but 5 of more than 14,000 requests for warrants to compel access to personal information.3

IMPLICATIONS FOR OUTSOURCING

The *US Patriot Act* has much greater international implications when one considers that most of the major IT firms which are capable of large-scale infrastructure services are US- based. IBM, EDS, and HP account for more than 40% of the market for enterprise IT outsourcing.4

IBM and EDS are understandably adamant that the personal information they acquire pursuant to outsourcing contracts is secure5. EDS points to the privacy provisions in its contracts, which it says are designed to protect the security of the individual's information, and the application of the *Privacy Act* to that information. According to a spokesperson for the company, if the US Government wanted Australian information for law enforcement purposes, EDS would take up the matter with the Australian authorities6.

The report by the Privacy Commissioner of British Columbia makes it clear that it would regard a disclosure of information by a US company of British Columbian personal information to be an offence under their local privacy legislation7.

In Australia, personal information is protected by the *Privacy Act*8. National Privacy Principle ("NPP") 2.1(e)9 provides for the primary duty of an organisation not to disclose personal information to a third party, unless it reasonably believes that such disclosure will lessen or prevent a serious threat to public safety. Note 1 of NPP 2 specifically provides that the non-

disclosure principle is not designed to deter law enforcement agencies from performing their function. It is unclear whether disclosure to a foreign law enforcement agency in order to lessen or prevent a serious threat to public safety, in Australia or elsewhere, falls within the scope of the exception.

NPP 9 provides that personal information may be transferred to a foreign country only if the organisation providing it reasonably believes that the recipient of the information is subject to a law which upholds principles for fair handling of information that are substantially similar to the NPPs. Even though the US is governed by its own federal privacy legislation10, the personal information, if handed to the US, would be governed by the *US Patriot Act*.

The US companies in Australia insist that they abide by the laws of the country in which they operate11. IBM recently stated that no personal information has in fact been disclosed by the company pursuant to the amended *FISA*12. Undoubtedly, commercial considerations act as a powerful incentive not to disclose personal information, and it is no surprise to hear the US companies loudly trumpeting their devotion to non-disclosure. However, it would not be too cynical to suggest that, if faced with considerable legal and political pressure from the US government, such devotion may be severely tested, and avenues of permitted disclosure explored. Significantly, if such information were obtained from the US companies in Australia under *FISA*, section 1861(d) would preclude the companies from disclosing this fact to any person. In addition, section 1861(e) relieves those who in good faith provide personal information to the FBI under an order from the

US Patriot Act: Implications For Outsourcing to US Companies

David Chan considers the *'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001'* and the potential for personal information in the possession of a US outsource provider to be disclosed to the FBI.

Recent announcements by the governments of South Australia and British Columbia that each is reviewing the effect of US anti-terrorism laws on their outsourcing policies highlights the difficulty that arises when local privacy obligations conflict with information gathering by government agencies.

The specific concern is that a US corporation with activities in a foreign country (say Australia) may be required, under the *US Patriot Act*1, to disclose personal information that is in its possession. This is of more immediate concern as in recent years large US corporations such as EDS and IBM have been providing much of our governments' IT infrastructure. For example, EDS currently handles the tax records of the Australian Taxation Office and most of South Australia's State government systems.

OUTSOURCING AND LAW ENFORCEMENT

The onward march of the digital age inevitably results in more and more personal information being stored "on-line" (actually on computer servers located elsewhere), and it's no surprise that law enforcement agencies have sought access to this vast information resource on grounds of national security. The growth of information technology outsourcing as a business strategy means that a government agency's files will now mostly be stored on servers owned by third party IT companies, just as the ISPs may outsource their storage to operators of server warehouses. Law enforcement agencies have consistently sought access to these third party systems but have until recently been restrained by a combination of civil libertarian persuasiveness and just plain old inertia. The events of September 11, 2001 overcame this inertia and in the US, the *US Patriot Act*, which was passed swiftly following the events of September 11, has given law enforcement agencies what they have long sought.

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Amid provisions which enhanced the powers available to US law enforcement agencies, the *US Patriot Act* also amended the *Foreign Intelligence Surveillance Act (US) 1978 Act* ("***FISA***"). The *FISA* is the act that gives US law enforcement agencies the power to access personal information. Prior to 1995 warrants were limited to electronic surveillance (e.g. wire taps) but in 1995 this was expanded to include the seizure of "certain records"2 (i.e. without the need for any surveillance).

The *FISA* also established a secret court, the Foreign Intelligence Surveillance Court, where law agencies are able to obtain orders giving them access to personal and private information. Section 1861(d) of the *FISA* makes it an offence for a person to even disclose to another person that personal information was sought or obtained by a law enforcement agency. As a result, the extent to which these activities are being carried out is almost impossible to ascertain.

Prior to the *FISA*, in order to obtain a warrant to compel access to personal information, the US enforcement agencies had to show that there was some evidence of wrongdoing. The *US Patriot Act* amendments to the *FISA* significantly relaxed this test. While section 215 of the *US Patriot Act* amended the *FISA* to allow US agencies to obtain records to protect against international terrorism and against clandestine intelligence activities, it also relaxed the test for obtaining a warrant. Whereas previously an applicant for such warrant had to show evidence giving reason to believe that the person whose records are sought is capable of being a foreign agent, now they only have to show that records are sought for the purpose of an authorised investigation into foreign intelligence not concerning someone who is a US citizen. Section 218 of the *US Patriot Act* further amends the *FISA* to relax the requirement that foreign intelligence gathering be the sole purpose for obtaining information. It now only has to be a "significant purpose".

Accordingly, a US law enforcement agency, such as the FBI, could obtain an order from the Foreign Intelligence Surveillance Court to compel a US company with operations in Australia to disclose information that it holds in its possession, so long as foreign intelligence gathering is a *significant purpose* for obtaining such information. It hardly seems that law enforcement agencies were

undertakings give competitors access to the content, albeit the whole pay tv packages rather than individual channels. Exclusive content agreements reward content producers, can reduce negative externalities and transaction costs and promote investment. Parties should be able to determine the commercial terms of access rather than have it dictated by legislation. There is no precedent in the FTA which requires commercial television broadcasters to onsupply programs or sporting events they have acquired and produced[45]. There are more cogent reasons why this situation should not be legislation in subscription television because of the unprofitable nature of the industry.

CONCLUSION

Although the Coalition has indicated no intention to divest Foxtel and/or the HFC network, the analyses provided above is useful should the government wish to revisit the matter in the future. Our discussion indicates a tension between economic and legal concerns. On the one hand, the government will aim to achieve the highest price for Foxtel shareholding and HFC cable, to ensure fairness for shareholders, and to reduce the possibility of government compensation. Invariably, this goal will deliver control of Foxtel and/or the HFC network to News Ltd and PBL. On the other hand, the structural separation of Foxtel from News Ltd and PBL decreases the need for government intervention but is not economically viable. Thus, to balance these competing considerations, we suggest a scheme whereby Telstra retains ownership of the HFC cable, while News Ltd and/or PBL increase its shareholding in Foxtel. Although the structural separation is incomplete, the current regulatory framework in the TPA is able to ameliorate most access concerns.

1 Australian Competition & Consumer Commission, report to Senator Alston, Minister for Communications, Information Technology and the Arts, "Emerging Market Structures in the Communication Sector", June 2003.

2 Alston R, Minister for Communications, Information Technology and the Arts, Media Release, "ACCC report on Pay tv competition". <http://www.dcita.gov.au/Article/0,,0_1-2_1-3_163-4_115441,00.html> (Accessed 28 September 2004)

3 Telstra's market power is demonstrated by its receipt of almost 60 per cent of total industry revenue, which is almost four times the revenue of its closest rival, Optus and it is reported to receive over 90 per cent of industry profits. See Note 1 at 30.

4 The Australian household penetration rate stands at 96.8 per cent. See Inquiry Into The Australian Telecommunications Network - Introduction And Preliminary Considerations., CEPU Submission.

<http://www.cepu.asn.au/comm.cepu/section_publications/submissions/sensub02.shtml>

(Accessed 3 October 2004).

5 Long R, Luciano M, "Aust/NZ Telecommunications Searching for a Signal" *Deutsche Bank Asia Pacific Equity Research Report*, 15 June 2004.

6 See note 1 at 39.

7 For example, unlike Optus, Telstra has not sought to supply telephony services on its HFC network which would reduce the revenue from its PSTN network. There is also scope for Telstra to develop its PSTN network to supply broadband and pay tv services.

8 Telstra Constitution (effective 14 November 2003), para 20.1.

9 Outgoing Telstra chief executive Ziggy Switkowski recently declared that his company's shareholding in Foxtel was "not negotiable". See Sainsbury M, "No sale of Foxtel, Telstra tells ALP", *The Australian*, 14 February 2004.

10 An estimated $550 million was been spent by Foxtel and Telstra, upgrading the HFC network, Foxtel televisions systems and set top units (STUs) to provide interactive content on digital tv. See Note 5 at 42 .

11 *Telstra Corporations Act 1991*.

12 The power of Telstra directions is limited by the *Telstra Corporations Act 1991* under the Telstra Constitution (effective 14 November 2003), para 20.2.

13 The only limitation on the power is that the Minister cannot give a direction in relation to the amounts to be charged for work done or services supplied by Telstra.

14 Telstra Annual Report 2004, 143.

15 These include the duty to act with "care and diligence" (s 180 *Corporations Act 2001)*, "in good faith in the best interests of the corporation" (s 181 *Corporations Act 2001)*, and not for an "improper purpose" (s 182 *Corporations Act 2001)*. See Garland J, Stapledon G, Watts T, Separating Telstra: Protecting the Interests of Minority Shareholders, Commissioned by the Chifley Research Centre, *Institutional Analysis Pty Ltd*, January 2003.

16 Austar United Communications Submission to the ACCC Report on Emerging Market Structures in the Communications Sector, Aug 2003 < http://www.dcita.gov.au/download/0,2720,4_116126,00.doc>

(Accessed 20 September 2004).

17 Meridian Connections Submission to the ACCC Report on Emerging Market Structures in the Communications Sector, 30 July 2003 <http://www.dcita.gov.au/download/0,2720,4_116125,00.doc>

(Accessed 20 September 2004).

18 See note 16.

19 *Trade Practices Act 1974* (Cth), hereinafter "*TPA*".

20 s 4G *TPA* states that the term "substantially lessen competition" includes "preventing or hindering competition".

21 Telstra would have incentives to invest and upgrade copper access network to provide broadband services and pay tv service. The market power of Telstra will be diminished as the opportunity to bundle Foxtel with Telstra is reduced.

22 Ferguson A, "Ziggy's last chance", *Business Review Weekly*, 8 July 2004.

23 Foxtel Submission to the ACCC Report on Emerging Market Structures in the Communications Sector, 24 Sep 2003 < http://www.dcita.gov.au/download/0,2720,4_116067,00.pdf>

(Accessed 20 September 2004).

24 News Ltd is the largest newspaper proprietor and magazine publisher in Australia while PBL owns the highest rating FTA broadcaster, the Nine Network. News Ltd and PBL are major content providers with ownership in the following producers: Fox Sports (50/50 News Ltd/PBL), XYZ (50/50 Foxtel/Austar), Fox Studios (News Ltd), NRL (50% News Ltd). See Seven Network Submission to the ACCC Report on Emerging Market Structures in the Communications Sector, 13 Nov 2003

http://www.dcita.gov.au/download/0,2720,4_116186,00.pdf>

(Accessed 20 September 2004).

25 There are three cross media ownership provisions relating to being in a position to exercise control of a commercial television broadcasting license, a commercial radio broadcasting license and a newspaper in the same area. *Broadcasting Services Act:* s 60.

26 See note 1 at 56.

27 *Broadcasting Services Act 1992*.

28 News Corporation Information Memorandum in relation to a proposal to "re-incorporate" in the United States and to acquire from Murdoch family interests their shareholding in Queensland Press Pty Limited, 15 September 2004.

29 Additionally, a foreign person must not have company interests in a subscription television broadcasting licence that, when added to the company interests in that licence held by other foreign persons, exceeds 35 per cent.

30 The foreign ownership limit is a test that applies to company interests rather than the degree of actual control exercised by foreign persons. News Ltd may have to adopt creative corporate restructuring, even if it does not increase its shareholding in Foxtel because it currently owns 25 per cent.

31 *Foreign Acquisitions and Takeovers Act 1975* (Cth).

32 *Foreign Acquisitions and Takeovers Act 1975* (Cth): s 19

33 Butler D, Rodrick S, *Australian Media Law* 1st ed (Law Book Co., 1999) 597.

34 Wright S, "Update: Telstra Awaits Vote, Ready To Talk With Labor", *Dow Jones Newswires*, Monday September 27 2004 <http://asia.news.yahoo.com/040927/5/1ow4i.html> (Accessed 30 September 2004)

35 Foxtel has paid hundreds of millions of dollars in licence fees for its movie channels. It has been reported that Optus has Hollywood movie content liabilities worth $300 million. See note 22.

36 See note 23.

37 ACCC, Deeming of Telecommunications Services, p.iv (Table A),152.

38 Foxtel was granted an exemption from the *TPA* that meant the ACCC could not regulate how it opened its digital platform to third parties until 2015. Under s 152ATA, the *TPA* enables an access provider to apply for an exemption from the standard access obligations before an investment in a telecommunications service is made or that service becomes an active declared service.

39 "The channel's reserve price is $750,000 a year and it's estimated accessing Foxtel's set-top box infrastructure would cost a would-be pay tv channel operator about $250 a subscriber. In addition, a channel operator would need to have tv-production facilities to produce content as well as its own customer call centres and billing operations. Industry sources say that all up, running just one channel would cost at least $35 million...also...any new channel would not be included by Foxtel in its basic digital package, meaning the channel operator would have to market and advertise the channel to prospective subscribers itself": Nicholas K, "Seven, Ten 'no' To New Channels" , *Australian Financial Review*, 12 May 2004.

40 Catalano C, "Pay tv ruling in Seven's favour", *The Sydney Morning Herald*, 1 October 2004.

41 Grant A (Ed), *The Communications Law Centre Guide Australian Telecommunications Regulation* 3rd Ed (UNSW Press, 2004) at 113.

42 See note 40.

43 s 87B of the *Trade Practise Act 1974 (TPA)* provides that the ACCC is able to accept a written undertaking in relation to a matter which it has power under the *TPA*. Undertakings given under s 87B are court enforceable through the ACCC applying to the Court when it considers the undertaking has been breached. Orders the Court may given include compensation and damages in addition to any other order that the court considers appropriate.

44 Optus Submission to the ACCC Report on Emerging Market Structures in the Communications Sector,07 Aug 2003

<http://www.dcita.gov.au/download/0,2720,4_116267,00.doc>

(Accessed 20 September 2004).

45 See note 44.

University student Daniel Yap is the Winner of the 2004 CAMLA Essay Prize Competition.

Defamation Law and the Fairness of the Objective Test

Sarah Krasnostein, highly commended in the 2004 CAMLA Essay Prize, discusses whether it is appropriate for defamation law to apply objective tests to determine liability in circumstances where the meaning of the text is subjective.

The law of defamation is particularly concerned with constructing meaning. This occurs at two stages. First, when determining the meaning of the contested words, the law "mimic[s] the ordinary publishee's response"[1]. Second, when determining whether that meaning is defamatory, the law anticipates the reaction it will elicit. However, both stages assume an idealised homogeneity of reader response in a society that is fundamentally heterogeneous in terms of, inter alia, age, language, ethnicity, experience and morality. If meaning is subjective, is it fair for defamation law to have such objective tests for determining the meaning of an imputation and whether it is defamatory?

IMPUTATIONS: MEANINGS AND DEFAMATION

The meaning of an imputation is determined by asking "*what an ordinary, reasonable publishee would understand from the material*"[2]. This question is, however, fundamentally at odds with postmodern literary and cultural theory which denies objectivity and the possibility of a homogenous reader response to a particular text. Current literary theory seems focused on asking, "What is the meaning of a text?" and "Is objective understanding possible, or is all understanding relative to a reader's particular situation?"[3]. Possible legal liability for defamation rests on the law's answers to these seemingly academic questions.

The same philosophical problems plague the second test for determining whether an imputation is defamatory. While there is no comprehensive definition provided by the case law, the suggested tests assume the same unrealistic homogenous reader response by asking "would the words tend to lower the plaintiff in estimation of right-thinking members of society generally?"[4]. Yet, while literary theories highlight problems with the way the law constructs meaning, they offer no pragmatic solutions to redress the clash of rights[5] at the heart of defamation law. Perhaps their value lies in highlighting alternative ways of understanding imputations, thus encouraging judges and juries to proceed self-consciously in selecting and justifying a text's dominant meaning and effect. This would be useful in exposing and understanding the policy behind defamation decisions by explicitly articulating why the right to reputation will sometimes trump freedom of speech.

TEST FOR DETERMINING MEANING

Unlike postmodern literary theory, the legal approach to determining the meaning of an imputation emphasises points of convergence in our understanding of language. These shared understandings come from living together in a liberal-democratic society. However, the impact of cultural differences on understanding may be relevant in that the term 'imputation' includes non-literal meanings. Natural and ordinary meanings (as distinguished from legal innuendoes) may not be 'natural and ordinary' to many in the community. This type of imputation is conveyed by inference. Such inferential meanings are called 'popular' or 'false' innuendoes and "depend on general community knowledge, such as knowing a common slang expression". However, given the diversity of the community, cultural and language barriers mean that slang may not be common and that certain types of knowledge may be absent in large sectors of the community.

Consequently, the role of evidence in determining meaning seems lacking.

In *United States* v. *Maxwell*23, the U.S. Court of Appeal for the Armed Forces affirmed that a person has an objective expectation of privacy in messages stored in computers which can be retrieved through the use of an assigned password. People also have an objective expectation of privacy with regard to messages transmitted electronically to other subscribers of the service who also has individually assigned passwords24.

This personal privacy expectation has been protected and demonstrated in title 39 of U.S. Code of Federal Regulations, Postal Service:

> "*No person in the Postal Service except those employed for that purpose in dead-mail offices, may open, or inspect the content of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise nonmailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.*"25

In effect, email is a form of letter. It is sent and sealed by a computer until the recipient retrieves it from his or her mail server. Hence, the sender and the recipient should enjoy the same expectation of privacy in their email as they would expect with their regular mail. That is, the mail will not be inspected by anyone unless there is a search warrant. Based on the same logic, electronic communications service providers, such as ISPs, should not allow access to theft clients' stored emails except under certain circumstances permitted by laws.

EMAIL PRIVACY BILL

To address the unfavourable consequences resulting from this juridical interpretation and the associated loose stipulation of the *Stored Communication Act*, on July 22, 2004, U.S. Congress sponsored the bill for the "*E-mail Privacy Act of 2004*."26 26 According to the summary of the bill, the objective of the Act is to modify the definition of "intercept" to include the acquisition of the contents of the communication through the use of any electronic, mechanical, or other device, at any point between the point of origin and the point when it is made available to the recipient. This Act also serves to limit the service provider exception to the prohibition on unlawful access to stored communications. Once the bill is enacted, emails that are in transit or in transit with contempor-aneously storage cannot be legally monitored without a wiretap order.

1 373 F.3d 197 (1st Cir., 2004)

2 18 U.S.C. § 2511: Interception and disclosure of wire, oral, or electronic communications prohibited: (1) Except as other wise specifically provided in this chapter [18 USCS § 2510 et seq.] any person who –

(a) intentionally intercepts, endeavours to intercepted or procures any other person to intercept or endeavour to intercept, any wire, oral, or electronic communication;

(c) intentionally discloses, or endeavours to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(3) (a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

3 *Electronic Communications Privacy Act* was divided into Title I, 18 U.S.C. 2510-2522, commonly known as the *Wiretap Act*, and Title II, U.S.C. 2701-2711, commonly known as the *Stored Communications Act*.

4 Supra note 1, 200.

5 Ibid 201.

6 *The Electronic Communications Privacy Act* Title II, U.S.C. 2701-2711, commonly known as the Stored Communications Act.

7 18 USC § 2510 (12): "electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system.

8 18 USC § 2510 (1): "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged in providing or operating such facilities.. .and such term includes any electronic storage of such communication. .." However, the Congress deleted the phrase "and such term includes any electronic storage of such communication" in 2001.

9 Ibid

10 Ibid

11 135 F. Supp. 2d 623 (E.D.Pa2001)

12 Ibid 633

13 Ibid 635

14 Ibid 636

15 Supra note 1, Dissenting Opinion 208-209. 16 ibid 219-220

16 Ibid 219-220

17 18 U.S.C. 2516-2518

18 18 U.S.C. 25 15

19 18 U.S.C. 2703(a)

20 Erich Luening, 'FRI takes the teeth out of Carnivore's name', CNET news.com, 9 February 2001, at: http://news.com.coml2lOO-l023-252368.html (last visited September 28, 2004)

21 18 U.S.C. 2701: (a) Offense. Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C. 2701 (c) (1): "exceptions. Subsection (a) of this section does not apply with respect to

conduct authorized (1) by the person or entity providing a wire or electronic communications service."

22 Robert A. Pilcowsky, 'The need for revisions to the law of wiretapping and interception of email' (fall 2003) 10 *Michigan Telecommunication and Technology Law Review* 47

23 42 M.J. 568 (A.F. Ct. Crim. App., 1995)

24 Ibid 577

25 C.F.R. 2333 (g)(1)

26 II.R.4956

University student Yi-Jen Chen received a Highly Commended Award in the 2004 CAMLA Essay Prize Competition. Yi-Jen Chen is a M. Phil Candidaate at the TC Beirne School of Law, University of Queensland.

plaintiff drafted a letter warning that agents might leave defendants over objectionable policies, the defendants searched Nationwide's electronic file server for email communication indicating whether the letter had been sent. The defendants opened the stored email of Fraser and other agents and found an exchange of emails between Fraser and an agent of Nationwide's competitor. The plaintiff alleged that the defendants' actions were in violation of the *Wiretap Act*. The plaintiff also asserted that the defendants unlawfully accessed his email from storage, in violation of the *Stored Communications Act*.'12

The Court held that,

> "*interception of a communication occurs when transmission is interrupted, or in other words when the message is acquired after it has been sent by the sender, but before it is received by the recipient.*"13

To clarify the concept of "intercepting email," the Court began with the discussion of the way email works.

> *"E-mail is stored in two different types of storage during the course of transmission - intermediate storage and back-up protec-tion storage. Retrieval of an e-mail message from either intermediate or back-up protection storage is interception; retrieval of an email message from post-transmission storage, where the message remains after transmission is complete, is not interception.*"14

In this case, the defendants acquired the plaintiffs email by retrieving it from Nationwide's electronic storage. At the time, the email had already been received by the recipient. The defendants did not retrieve the email before it was received and read by the recipient, and therefore, the Court concluded that there was no "interception."

The Government's contention in the *Councilman* case was consistent with the *Fraser* court's approach. According to the Government,

> "*an intercept is subject to the Wiretap between the time that the author presses the 'send' button and the time that the message arrives in the receipt's email box. Accordingly, the Wiretap Act should apply to message that are intercepted contemporaneously with their transmission and the Stored Communication Act would apply to messages that are accessed non-contempor-aneously with transmission.*"15

The Government's contention in *Councilman* and *Fraser* are theoretically consistent with the *Wiretap Act*. The decision in the *Councilman* case will ultimately have detrimental effects on the protection of personal privacy and security.

The most serious adverse effect of the *Councilman* case is that law enforcement officers could follow the less legal procedure with less juridical supervising for interception of electronic communications16. Under the *Wiretap Act*, only certain federal felonies are allowed to be wiretapped. To obtain a wiretap order, the officers must make a statement including a description of the offence, the location of the communications, the type of communications, and the identity of whose communications are to be intercepted. The judge may require the officers to furnish additional testimony or documentary evidence in support of the application. If necessary, the court could require reports showing the progress made toward achievement of the authorized objective and the need for continued interception.17 Most importantly, any content of communication intercepted in violation of the rules made under the *Wiretap Act* cannot be received in evidence.18 In contrast, those procedural protections under the *Wiretap Act* are not applicable to the *Stored Communications Act*. Law enforcement officers could gain access to contents of any wire or electronic communications in electronic storage simply by obtaining a search warrant.19

Pursuant to *Councilman's* narrow interpretation of the *Wiretap Act*, law enforcement officers no longer need to obtain a wiretap order to monitor email accounts. For example, the U. S. Federal Bureau of Investigation ("**FBI**") designed a system, Carnivore, to monitor the Internet communications of suspects under its surveillance. However, the system, housed on computers at Internet service providers, can also collect email messages from people who are not under its investigation.20 From the view point of the *Councilman* court, FBI agents would be free to install the system into ISPs' servers to monitor all web surfing and email that are temporarily stored in electronic routers during transmission without complying with the strict procedural provisions in the *Wiretap Act* for seeking a wiretap order.

Besides the flaw of the *Councilman* court's ruling, section 2701(a), coupled with section 2701(c)(l) of the *Stored Communications Act*21, exempt an electronic communication service provider from the prohibition against unlawful access to stored communications. Without the restrictions of the *Wiretap Act* and the *Stored Communications Act*, ISPs have the right to invade the privacy of their clients' electronic communications for any reason and at any time. Personal privacy on the Internet could be easily invaded.

Since a privacy right is created by law, the protection should be the same regardless of the medium of communication. Letters in the postal communication, telephone conversations, and email should all receive the same level of protection from surreptitious interception by law enforcement officers or private parties. People's interest in their privacy of the emails is the same as their privacy interest in a telephone conversation and the mail.22

Readership surveys are not admissible, as they would erode the jury function to apply the test of the ordinary, reasonable recipient. However, such surveys could correct jury members' assumptions about the generality of certain types of knowledge. This point is subtly acknowledged by the law in making relevant the general manner and occasion of publication. Importantly, the publication's context can include the class of likely publishees. This allows consideration of "*the person or class of persons whose reaction to the publication is the test of the wrongful character of the words used*"[6]. Attention to "*the kind of person who will receive the communication in question*"[7] provides a narrower objective test. This is closer to the justice of subjective consideration of what was actually interpreted.

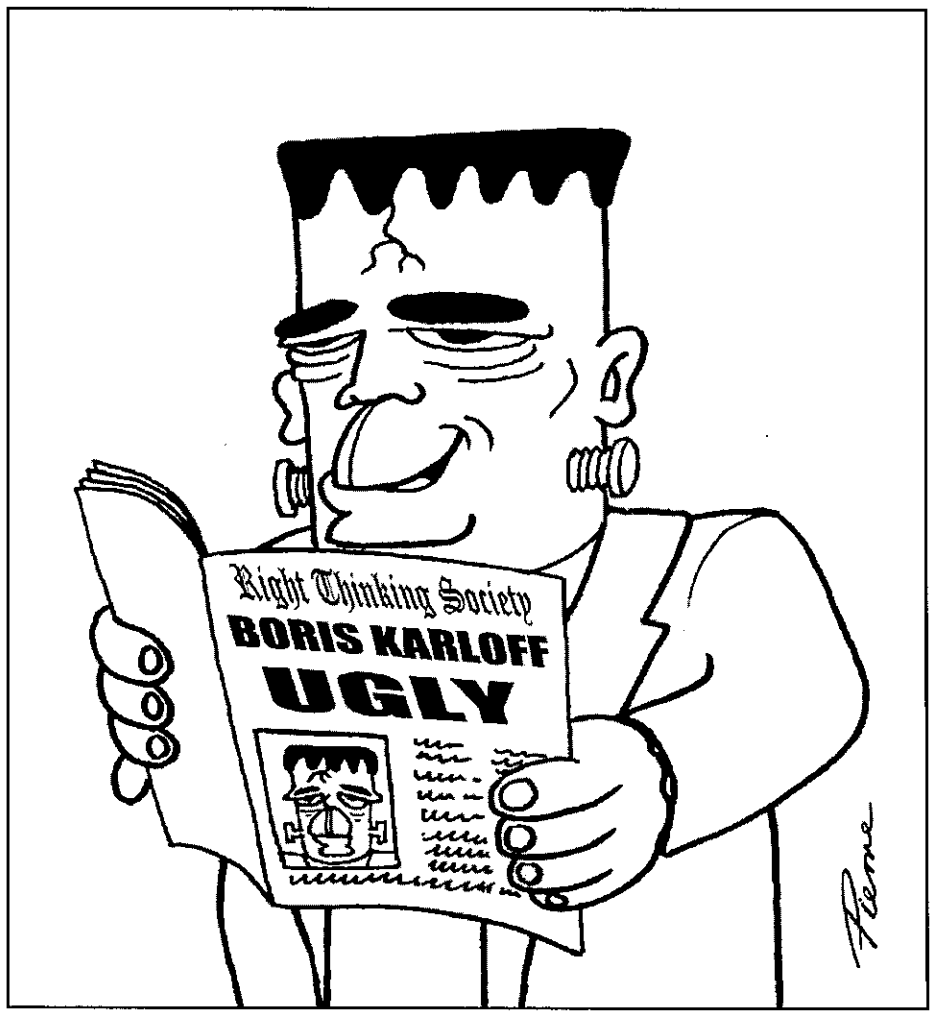
It seems strange that the question of whether the text is capable of conveying an imputation is characterised as a question of law when it concerns significant questions of fact. Further, reserving this question of fact for the judge can promote injustice because, in many instances, it is fundamentally connected to mainstream popular culture and average community norms. The ability of judges to fulfill this role is called into question by the Honourable Justice Kirby himself stating that:

> "*Some would consider it presumptuous for judges (many of who lead narrow lives...) to assert that they know what reasonable fellow citizens will make of a broadcast*"[8].

Currently limited to deciding whether a meaning is actually conveyed, the jury is arguably better placed than the judge to determine realistically (and fairly) whether a text is capable of conveying an imputation.

TEST FOR DETERMINING WHETHER A MEANING IS DEFAMATORY

Problems with the objective test similarly arise in the next stage of determining whether the decided meaning is defamatory. The law's



recognition that meaning changes over time because it is socially constructed is important to determining whether an imputation is defamatory. Thus, it was once considered defamatory to call someone a communist or a homosexual. However, this concession to the malleability of meaning is not extended across society to acknowledge that reactions to an imputation can change between different groups of people at the same time.

The various judicial approaches determine that the imputation relied on must be likely to cause "*ordinary decent folk in the community*"[9] (also described as "*right thinking members of society*"[10]) to think less of the plaintiff. However, in the absence of a subjective test or evidence for determining what the reaction actually was, it seems that this results in a finding of what people should think, rather than what they actually did[11]. Given the differences in our society, what exactly is "right-thinking"? By not making the variety of possible reactions explicit, judges expose themselves to criticism of biased policy choices determining outcome, rather than a realistic determination of majority reaction[12]. This is illustrated by the case discussed by Barendt, *Mycroft v Sleight*, where the court denied the plaintiff, a trade union official, damages in respect of an allegation that he had worked during a strike. However reactions to this imputation could have ranged from indifference to approval to anger "causing other persons to 'shun or avoid'" the plaintiff[13]. By finding that the claim had not damaged his reputation, the court made an ideological decision about the "right" reaction and subsequently which sectors of society are justly considered "right-minded" or "decent".

This control over the meaning of words and the value of the reactions they elicit is cloaked under the objective claims of defamation law. However, disagreement between judges sitting on defamation cases shows the frailty of this fiction. The dissent by Millet LJ in *Berkoff v Burchill* demonstrates the malleability of meaning and,

subsequently, how tenuous a finding for legal liability for defamation can be. His Honour duplicates the defendant's contested statement by stating

> "*It is common experience that ugly people have satisfactory social lives – Boris Karloff is not known to have been a recluse...*"

He goes on to conclude

> "*if I have appeared to treat Mr Berkoff's claim with an unjudicial levity it is because I find it impossible to take seriously.*"

This is a serious contrast to Niall LJ's finding that the statements were

> "*capable of lowering his standing in the estimation of the public and of making him an object of ridicule*".

When the court cannot agree on the reaction to a statement, the subjectivity of meaning and variety of legitimate reactions to a text is demonstrated highlighting problems with the objective test.

CONCLUSION

Defamation law addresses the painful co-existence of freedom of speech and the "*interest all individuals have in safeguarding or vindicating their reputation*"[14]. Postmodern literary theory could make a valuable contribution to the law by encouraging claims to objectivity in meaning to be disregarded and the policy justification for erring on one side or the other to be made explicit. This would result in a clearer understanding of the uses of defamation law in society.

1 Andrew Kenyon, Media Law 2004: The Australian Plaintiff's Case, Melbourne University Course Material, 50.

2 Ibid.

3 See Terry Eagleton, *Literary Theory: An Introduction* (1983) 66.

4 *Sim v Strech* [1936] (Lord Atkin).

5 See Eric Barendt, 'What is the point of libel law?' (1999) 52 *Current Legal Problems* 110, 111-117.

6 *Sim v Strech* [1936] (Lord Atkin).

7 *Chakravarti v Advertiser Newspapers* [1998] (Kirby J).

8 *Bond Corp Holding v ABC* (1989) (Kirby J)

9 *Boyd v Mirror Newspapers* [1980] (Hunt J)

10 *Sim v Strech* (Lord Atkin)

11 See Lyrissa Barnett Lidsky, *Defamation, Reputation and the Myth of Community*, *Washington Law Review* (1996) 9.

12 See Ibid.

13 *Morgan v Lingen* (1863), *Yousoupoff v MGM* (1934).

14 Barendt, above n 5, 112.

University student Sarah Krasnostein received a Highly Commended Award in the 2004 CAMLA Essay Prize Competition.

Invasion of Electronic Communication Privacy

Yi-Jen Chen, highly commended in the 2004 CAMLA Essay Prize, considers the impacts of the recent decision of the United States Court of Appeals for the First Circuit in *United States of America v Branford C. Councilman*

With the rapid development of computer technology, individuals are becoming increasingly dependent on the Internet to communicate and conduct their every-day business activities. While the Internet has promoted greater access to public and private services, it has raised new concerns regarding personal privacy and security. Online users' communications, for example, may now be exposed to the wider public. Any person who has superior computer knowledge, or who employs particular software, could easily monitor other users' activities on the Internet. The legality of employers' and internet service providers ("**ISP**") monitoring online users' electronic communications, such as the use of electronic mail, instant messaging, forums and bulletin boars, has been discussed vigorously. On 29 June 2004, the ruling made by the United States Court of Appeals for the First Circuit in *United States of America v Branford C. Councilman1* focused significant attention on the issue of electronic communication privacy. According to this decision, ISPs have the right to read and copy the inbound email of their clients.

THE COUNCILMAN DECISION

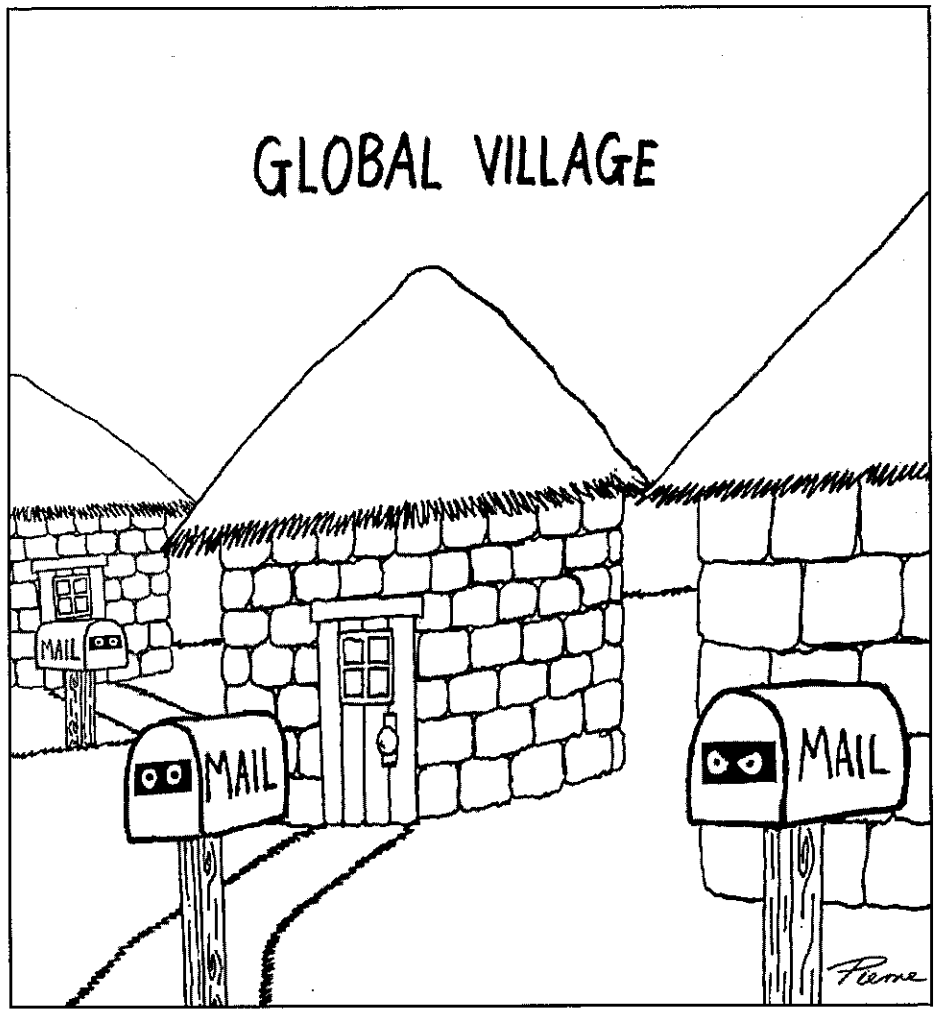
In the *Councilman* decision, the defendant was the Vice President of Interloc, Inc. ("**Interloc**"). Interloc is an ISP, which provides an online rare and out-of-print book listing service and email service for its clients. The defendant was accused of directing Interloc employees to write computer codes (procmail.rc or "the **promail**") to intercept and copy all incoming emails from Amazon.com before they were delivered to the clients. The employees were also instructed to read these emails to gain commercial advantage. The defendant's action allegedly violated sections 2511 (1)(a), (c) and 2511 (3)(a)2 of the *Electronic Communications Privacy Act* ("***Wiretap Act***"3). The violation included intentionally intercepting electronic communications, disclosing the contents of the intercepted communications, and causing a person to divulge the contents of the communications while in transmission to persons other than the addressee of the communication4.

The issue was whether there was an "intercept" of a communications within the meaning of the *Wiretap Act*5. In the email transfer protocol, an email message is locally stored, formatted and forwarded by mail transfer agent ("**MTA**") through the Internet from one MTA to another until it reaches the recipient's mail server. Once the message reaches the recipient's mail server, a mail delivery agent ("**MDA**"), which in the *Councilman* case was a program called "promail", will retrieve the message from the MTA, determine which user should receive the email and place the message in the user's mailbox. In the process of retrieving and placing, the message is temporarily stored in the random access memory ("**RAM**") or on hard disk within the ISPs computer system. In other words, an email is stored contemporaneously with it transmission.

Accordingly, the defendant argued that the email interception in this case was defined in the *Stored Communications Act*6. It was in a form of "electronic storage" and could not be intercepted in violation of the *Wiretap Act*. The defendant's submission was favoured by the United States District Court for Massachusetts and upheld by the Court of Appeals.

In dismissing of the indictments, the *Councilman* court focused on the differing definitions of "wire communications" and "electronic communication" in the *Wiretap Act*. According to the Court, the definition of "electronic communications" in section 2510 (12) of the *Wiretap Act*7 fails to provide for any "electronic storage". In contrast, "wire communication" included "any electronic storage of such communication" in its definition8. The omission of "electronic storage: in "electronic communications" was intentionally excluded by the Congress from applying "intercept" to "electronic communications" when those communications are in electronic storage. In order to find an offence against the intercept provisions of the *Wiretap Act*, interception must take place,

> "*when the message is... 'in transit' or 'in process of delivery'. No interception can occur while the emails are in electronic storage and therefore, without the requisite interception, the Wiretap Act could not be violated.*" 9



Since the electronic communications in this case were in a form of electronic storage, the Court of Appeal affirmed that no interception occurred and the case was dismissed. Accordingly, the *Councilman* decision indirectly indicated that email providers can copy and read the email of their clients.

COUNCILMAN AND THE WIRETAP ACT

Applying the *Councilman* approach, the *Wiretap Act's* prohibitions against "intercepting" electronic communication would be virtually invalid for the following reason.

> "*All digital transmissions must be stored in RAM or on hard drive while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an email message must store those packets in memory while it reads their addresses, and every digital switch that makes up the telecommunications network through which the packets travel between computers must also store the packets while they are being routed across the network...*
>
> *Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.*"10

Before the *Councilman* case, the U.S. District Court for the Eastern District of Pennsylvania had confronted the issue of the intersection of the *Wiretap Act* and the *Stored Communications Act* regarding the interception of email. In *Fraser* v. *Nationwide Mutual Insurance Co.*,11 the plaintiff, Fraser, was an agent of the defendant insurance companies. After the