of *The Panel* said:

> *The set was a little.....*
>
> *Perplexing.*
>
> *It was sort of like the seats were 'Who Wants to be a Millionaire' meets the desks of 'The Footy Show' meets an inner-city brothel. It was just....what I imagine an inner-city brothel would look like is what I mean.*

Justice Conti considered that there was not a viable basis for criticism or review and that the members of *The Panel* were just trying to be amusing. In fact, he commented that there was not 'a viable basis for comprehending, much less resolving, what was the true nature of the criticism.'

**Sufficient acknowledgement**

Both defences require that sufficient acknowledgement of the author of the work is given before the defence can be established. Justice Conti commented that this is ordinarily achieved by communicating, by spoken words or writing the authors' name. He held that use by Ten of an 'on-screen watermark 'Ch 9" was sufficient acknowledgement even in the absence of Nine's logo being shown.

## WHAT DOES IT MEAN FOR BROADCASTERS?

Based on Justice Conti's judgment, taking small parts of a competitor's broadcast programs, or segment of a program, will generally not be an infringement of copyright so long as the excerpt is not used for a commercial purpose, or to damage a competitor's interests. A practical test for broadcasters will be to ask if there has been a commercial pirating, in the sense that harm has been inflicted, or potentially will be inflicted, on the television broadcaster's commercial interest in the program. If there has then it is likely that there has been a substantial taking. An assessment of the quality and quantity of the excerpt is still essential, but the purpose element will be significant in determining the final outcome.

A word of warning, however - although certainly providing a level of comfort, there is no guarantee that Justice Conti's interpretation of sections 25(4)(a) and 87 will be followed, and , therefore, the use of a small (insubstantial) part of a competitor's broadcast (where the fair dealing defence is not available) may still carry with it some risk.

The fair dealing defences will be available despite the program having a primarily humorous or satirical focus. The defence of reporting the news is not restricted to serious commentary, however it must be clear that it is news and not entertainment, a distinction which is often difficult to draw. If the criticism or review is genuine then the commentary need not be balanced, or serious. However hidden commercial motives may disqualify a broadcaster from relying on this defence, particularly if they are a trade rival using the copyright subject matter for their own benefit. These issues will be a question of degree and impression, and, ultimately, what sense of humour the court thinks a fair and honest minded person has!

***Tim Golder is a Partner and Teresa Ward is an Articled Clerk at the Melbourne Office of Allens Arthur Robinson.***

# M-Commerce and Wireless Advertising – Legal Challenges for Carriers

**Buying a coke with your mobile phone is just the beginning for mobile commerce, Niranjan Arasaratnam and Joanna Davidson discard the hype to assess this new service.**

The mobile commerce reality finally caught up with the hype in Australia in May. Coca Cola installed nine vending machines at Sydney's Central Station which allowed consumers to "dial a Coke" using their Telstra mobile phones and have the cost of the drink added to their phone bill. The phrase "Dial a Coke" was added to the suburb display on the screen of phones which have the location display option enabled, reminding consumers that the service is available. This initiative represents only the most miniscule tip of the mobile commerce iceberg.

Mobile location services are value-added services that are based on a consumer's location. They combine three factors that boost the value of information to the typical consumer: personality, time-criticality and location-dependency. They have the potential to provide solid revenue streams to carriers in mobile markets where voice telephony revenues are reaching saturation point.

Interestingly enough, regulation is driving the development of mobile location services internationally. For example, in both the US and the EU, legislation mandates carriers to provide emergency services location information in the near future. This has had a significant impact on the positioning technology adopted by mobile network operators.

Developments in mobile location service technology raise some unique privacy concerns. Regulators in overseas markets are paying increasing attention to such concerns. In Australia, with the new privacy legislation on the horizon, the regulation of this technology is at an embryonic stage.

## A UNIQUELY SENSITIVE TECHNOLOGY

Mobile location services carry with them some novel legal issues. In particular, the major privacy concerns of the wired internet (including surveillance, spam and profiling) are magnified by wireless technology. It allows carriers to form a

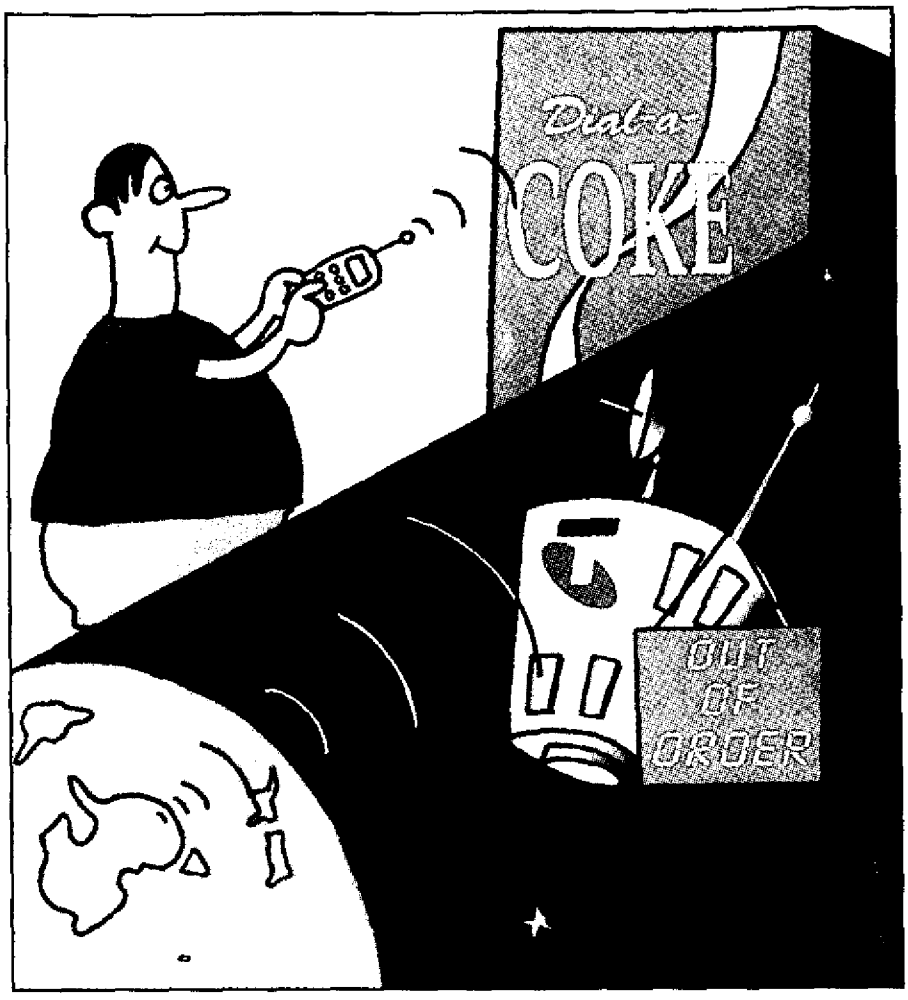
detailed and invasive dossier of each customer's movements (coupled with the government's increasing enthusiasm for surveillance technology as evidenced by the recent *Cybercrimes Bill 2001*). However, there are other legal challenges of the wireless environment, including:

- competition issues associated with interoperability of wireless platforms (eg refusal to roam, carrier collusion regarding APIs and market platforms);
- consumer credit compliance for carriers;
- legal recognition of wireless messages (eg the recent furore in Malaysia over whether SMS divorce declarations were valid under Islamic law);
- liability allocation issues (for example, what happens when a phone is stolen and used to fraudulently purchase goods?) and
- carrier control over advertising and other content carried on their network – should carriers have responsibility and act as a clearinghouse for advertisers, or should the ISP model apply, whereby ISPs act as mere conduits and content control is not assumed?

## WHAT REGULATORY ACTIVITY IS HAPPENING OVERSEAS?

The regulation of mobile location services is generating a lot of steam in the US, where E-911 laws for emergency services location information are accelerating carrier timetables for technology implementation.

In a series of E911 orders since 1996, the Federal Communications Commission (FCC) has required that mobile phone carriers provide location information automatically to 911 call centres on calls from mobile phones. Under phase II of the E911 rules, wireless carriers must provide to call centres the location of a 911 caller by exact latitude and longitude. In most cases, phase II compliance must occur by October 1 2001, and by the end of 2005, carriers must achieve a 95% penetration of handsets capable of providing location information.




The *Wireless Communications and Public Safety Act* 1999 added location to the definition of customer proprietary network information (CPNI). The Act specifically addresses the use of wireless location information and requires that a carrier obtain a customer's "express prior authorisation" in order to use or disclose call location information concerning the user of a commercial mobile service. There is an exception for emergency-related disclosures where express prior approval is not needed.

Curiously, the privacy rules for CPNI were successfully challenged by carriers on constitutional grounds in the case of *U.S. West v FCC* in late 1999. The court held that the privacy rules infringed the carrier's freedom of speech. The FCC is redrafting its CPNI privacy rules to avoid constitutional issues. However, even those carriers who challenged the privacy rules have now petitioned the FCC to immediately develop location privacy rules. They argue that it is in the public interest and the interest of emerging location services providers to develop the privacy rules as soon as possible.

On July 11, the *Location Privacy Protection Act* 2001 was introduced into the US Senate. This Bill aims to further protect the privacy of location information by prohibiting all providers of location-based services from collecting, using, disclosing or retaining location information without the customer's express authorisation. It would also strictly control the use third parties could make of location information, even though they could only receive it pursuant to a customer's express permission. The third party would not be able to disclose or permit access to location information without direct permission from the customer. The Bill has been referred to the Senate Commerce Commission for consideration.

In the EU, a Draft Directive on privacy in the electronic communications sector includes a specific article on location

data. Under proposed article 9, location data may only be processed by electronic communications networks if it is made anonymous, or with the consent of customers only for as long as necessary to provide a value added service. Even if consent has been obtained, the customer must continue to have the possibility of temporarily refusing the processing of such data for each and every connection to the network or transmission of a communication. This must be a simple, free process.

The EU's Data Protection Working Party suggested in its Opinion on the Draft Directive that this is not a satisfactory solution to privacy risk. It said that the rule should be inverted: the customer should be able to allow the processing of location data for each delivery of an added value service, but the default setting should prevent the processing of location data at all. The discussions continue but the Draft Directive is expected to be passed by the European Parliament this September. By the end of 2001 the EU will also have received the results of a technical study currently being offered by tender on caller location in mobile networks.

Self-regulatory efforts overseas are also continuing apace. The US Cellular Telecommunications and Internet Association has proposed rules for fair location information practices to the FCC, based on the principles of notice, consent, security, integrity and technology neutrality. The Wireless Advertising Association has developed technical standards for size and graphics in SMS advertising, as well as a set of guidelines on privacy and spam. These impose particularly high standards for customer consent to "push" messaging, insisting on confirmed opt-in by subscribers to wireless advertising services.

## WHAT ABOUT AUSTRALIA?

In Australia, the Australia Communications Industry Forum (**ACIF**) has established a working committee to develop an SMS marketing code of practice amid rising complaints of unsolicited SMS messages. The working committee's brief covers specific rules of messaging and some privacy issues. It is unclear whether the code will be voluntary or registered with Australian Communications Authority (and binding).

ACIF has also developed a specification governing how mobile carriers should provide mobile location information for emergency services and the transport of that information by transit networks. The specification is voluntary but the ACA is drafting a new determination which will implement the specification.

In the absence of any other specific regulation, the changes to the *Privacy Act 1988* (or the ACIF code governing personal information if registered by the Privacy Commissioner as an approved privacy code) will apply from 21 December. The *Privacy Act* will prevent the use and disclosure of any location information without the consent of the customer. Based on the National Privacy Principle Guidelines issued by the Privacy Commissioner, a broad, general consent obtained upfront may not suffice for unsolicited mail. This means mobile carriers may not be able to use personal information to send SMS in the ways they want to. Consent to direct marketing must be *explicit* with the customer understanding the full extent of the proposed direct marketing. In the absence of a general consent, consent will be required for each specific use of the location information.

However, there may be a loophole in the Act that could be exploited by the telco industry. The *Privacy Act* governs the collection and use of personal *information ... about an individual whose identity is apparent, or can reasonably be ascertained, from the information.* Whether information such as mobile location will identify an individual will depend on the context and who holds it. If the mobile location information that carriers exploit is merely limited to location information (without any reference to a person's identity) it may fall outside the ambit of the *Privacy Act* allowing carriers to use it without restriction.

The concept of privacy is multi-faceted. One can apply the moniker of a privacy interest to several understandings of privacy, such as the right to have the moral freedom to exercise full individual autonomy, the right to control your personal data and the right to solitude, secrecy and anonymity. Mobile location services encroach upon all these privacy interests to some degree. The *Privacy Act*, however, only addresses personal data protection.

## CONCLUSION

Privacy concerns with mobile location services are not just a regulatory issue. In a recent survey conducted by The Yankee Group, over 50% of respondents registered a worry over location information misuse. A cavalier approach to privacy might lead to customer churn rather than increased revenues. It may also lead to a knee-jerk legislative response and possible over-regulation of this area.

The industry needs to take leadership and develop a self-regulatory model that reconciles fair location information practices with the right of carriers to exploit their information for legitimate business goals.

***Niranjan Arasaratnam is a Partner and Joanna Davidson is a research assistant at the Sydney Office of Allens Arthur Robinson.***