

## Smile, You're on Mobile Phone Camera

**Paul McLachlan takes a peek at the potentials for regulation of misuse of mobile phone cameras.**

The media have been reporting community concerns about the use of the digital cameras in the latest generation mobile phones to take pictures of people in gym lockerrooms. Many gyms have reportedly banned mobile phones from locker rooms. The Attorneys-General are considering whether they should regulate the use of the technology.

How does the law deal with this conduct already? Depending on who the picture is of, which jurisdiction they are in, and the circumstances of how it was taken (and distributed), there may be a variety of different legal actions.

### TELECOMS INTERCEPTION

The *Telecommunications (Interception) Act 1979* (Cth) deals with interceptions of communications passing over the telecommunications system. According to the Courts, the legislation intends both to protect the privacy of those communicating, as well as the technical integrity of the telecommunications system.<sup>1</sup>

Taking a photo with a mobile phone and simply storing the photo would not be an interception under the legislation. There is no communication that passes over the telecommunications system.<sup>2</sup>

Taking a photo with a mobile phone and then using the phone to send it to someone else, or upload it to the Internet, would also not breach the legislation because the Courts have interpreted the legislation such that a party to a communication cannot intercept the communication, especially when using equipment that is part of

the telephone system (such as an ordinary mobile phone handset).<sup>3</sup> The legislation protects the privacy of the parties communicating, not of those whom the communication is about. The privacy rights protected are those of the person taking and sending the picture, not the person in the picture; in the same way as the legislation would prevent bugging of a conversation in which the parties discuss a third party's private affairs, but not the disclosure and recording of the private affairs as between the parties to the call themselves.

### SURVEILLANCE DEVICES LEGISLATION

Each State and Territory has legislation dealing with civilian use of listening devices (devices that overhear or record private conversations).<sup>4</sup> Some have also updated their legislation to include other surveillance devices, including

visual surveillance devices (devices that show or record private conduct). A mobile phone that can take still pictures or short moving pictures would be an "optical surveillance device" in those jurisdictions that regulate them (Victoria, Western Australia and the Northern Territory).

It would be an offence under the legislation in those jurisdictions to take a photo of private activity if you are not a party to the activity or have a warrant, or have obtained the consent of the person engaging in the activity. In Western Australia, there is also the ability to use the device if it is reasonably necessary to protect your lawful interests or in the public interest (which, in the case of gym lockerrooms, seems unlikely).

However, there is a question of the extent to which the legislation applies. The *Telecommunications (Interception)*

### INSIDE THIS ISSUE

**Smile, You're on Mobile Phone Camera**

**Review of Online Sales Contracts**

**You Can't Stop the Music**

**Privacy Tort, Where Art Thou?**

**Casenote: *Cullen v White***

**Local Advertising on Regional Television**

**Casenote: *ATECO Automotive Pty Ltd v Business Bytes Pty Ltd***

**The Spectre of Change in  
Spectrum Management**

**Spam Bill Almost Law**

## CONTENTS

### Smile, You're on Mobile Phone Camera

Paul McLachlan takes a peek at the potentials for regulation of misuse of mobile phone cameras.

### Review of Online Sales Contracts

Simon Minahan considers issues relevant to risk-managed online sales to an international market, and examines how to minimise some of the risks inherent in the multi-jurisdictional, international marketplace of the internet.

### You Can't Stop the Music

Peter Mulligan examines music piracy and parallel importation issues in the context of the recent case *Universal Music Australia v ACCC*.

### Privacy Tort, Where Art Thou?

Gayle Hill compares the recent UK rejection of a tort of privacy with Australian developments in the area.

### Casenote: *Cullen v White*

Kerin Forstmanis looks at a recent damages award for defamation on the internet.

### Local Advertising on Regional Television

In this edited version of her paper presented at the Communications Research Forum 2003, Helen Wilson looks at the state of regional television, and the contrast between local news content on the one hand, and local advertising content on the other.

### Casenote: *ATECO Automotive Pty Ltd V Business Bytes Pty Ltd*

Nick Abrahams and Liong Lim review a recent decision of the New South Wales Supreme Court which provides some valuable insights for technology customers.

### The Spectre of Change in Spectrum Management

Tom Reid and Niranjana Arasaratnam discuss the Federal Government's proposal to merge the ACA and the ABA in light of some responses from industry and interest groups.

### Spam Bill Almost Law

John Corker examines the new proposed model for regulating spam in Australia, and critiques some potential problems.

*Act 1979* (Cth) appears intended to cover the field with respect to the regulation of interception devices used in conjunction with telephone equipment.<sup>5</sup> If something is permitted under the Commonwealth legislation, but forbidden under the State legislation, does the State legislation apply? The Commonwealth legislation expressly allows for a person to overhear a private conversation where it is detected using equipment that is part of the telephone system. The same would apply for a videophone that allows someone to see a third party's private activity at the other end (for example, in the background behind the other party to the conversation). But, where the phone must first be used as a camera and then separately used as a telephone to transmit the picture (ie, it is not real-time transmission of the conduct), this is likely to fall outside the Commonwealth legislation. There is probably scope, then, for the State video surveillance legislation to apply.

But, the device must allow the user to see or record private activity. Private activity is defined in the State Legislation as activity that the parties would reasonably have considered not capable of being seen. Unless in a private cubicle or an empty locker-room, undressing or showering in sight of strangers would not be private activity. Taking a photo secretly would most likely not be using a surveillance device to record private activity.

---

### PRIVACY ACT

---

The Privacy Act 1988 (Cth) is unlikely to offer protection. A photo of a recognisable individual may be "personal information". However, the Act only binds business entities.

---

### TORT

---

The High Court in *ABC v Lenah Game Meats*<sup>6</sup> signalled that there might be a tort of invasion of privacy in Australia. The District Court of Queensland

recently found the existence of such a tort and awarded substantial damages for an invasion of privacy.<sup>7</sup> According to that case, the tort requires the infliction of physical harm (such as mental or emotional harm) and an invasion of privacy that a reasonable person of ordinary sensibilities would find highly offensive. The decision is currently on appeal.

It is early days yet for the development of such a tort. There certainly seems to be a high degree of community concern about the use of these camera phones in locker-rooms, but whether the invasion of privacy will cause mental or emotional harm will be difficult to show in each case.

---

### DEFAMATION

---

While defamation protects a person's reputation, rather than their privacy, it is often used in cases where privacy has been invaded. There is already a precedent for someone taking action

based on covert photographs in a locker-room. Andrew Ettinghausen sued when grainy black and white photographs of him taking a shower in the changing rooms after a football game were published in a magazine. That case involved grainy full-frontal naked photographs without his consent. He was awarded \$100,000 damages.<sup>8</sup>

Using a mobile phone camera to take photos of somebody in the public eye does carry the risk of being sued for defamation if they are subsequently published. But, the difficulty is establishing how the picture defames the person; and it does not protect a person who has no substantial reputation or where the picture is taken but not published.

---

### OTHER CLAIMS

---

Depending on the circumstances, there could be a case for criminal stalking, intentional infliction of (mental) harm, extortion, child pornography, or even misleading and deceptive conduct. However, few of these strike at the initial conduct of taking the photo without knowledge or permission; they deal with subsequent publication or use of the images. None of them provides blanket protection against the use of cameras in locker-rooms.

---

### WHAT ARE THE A-GS TO DO?

---

The issues for the Attorneys-General to consider are broader than simply a ban on the use of these telephones in locker-rooms. It will not suffice simply to encourage all jurisdictions to extend their listening devices laws to visual surveillance devices (although that is a logical first step). Ultimately, this involves the convergence of technology and what is considered private. As technology becomes smaller, more sophisticated, easier to use and able to make an image available to millions instantly, community concern about what is considered private will grow. Rather than simply protecting what goes on in the privacy of the home or otherwise undetected behind closed doors, people are coming to expect what they do in public to be protected from surveillance and mass distribution. The



community test is more likely to be whether the person expected to be photographed and have their conduct published to the world-at-large, rather than whether they expected it could be detected at all. What you may be comfortable doing in front of a small number of strangers, you may not be comfortable doing in front of millions.

*Paul McLachlan is a Senior Associate at Malleons Stephen Jaques in Brisbane.*

1 See R v Edelsten (1990) 21 NSWLR 542 (NSW Court of Crim Apl) T v Medical Board of SA (1992) 58 SASR 382 (SA Full Ct) and Green v R (1985) 135 ALR 81 (WA Court of Criminal Appeal).

2 Section 6(1).

3 Green v R (above); R v Evans & Doyle (1999) 152 FLR 352 (Vic Sup Ct).

4 Surveillance Devices Act 1999 (Vic), Surveillance Devices Act 1998 (WA), Surveillance Devices Act 2000 (NT), Invasion of Privacy Act 1971 (Qld), Listening Devices Act 1984 (NSW), Listening Devices Act 1991 (Tas), Listening Devices Act 1992 (ACT), Listening & Surveillance Devices Act 1972 (SA).

5 Miller v Miller (1978) 141 CLR 269; Edelsten v Investigating Committee of New South Wales (1986) 7 NSWLR 222.

6 (2001) 185 ALR 1.

7 Grosse v Purvis [2003] QDC 151 (unreported).

8 Ettinghausen v Australian Consolidated Press Ltd (1993) A Def R 51-065.