There were also debates during the passage of the Digital Agenda Act about the appropriate scope of the definition of "technological protection measure". Unlike in the US, the definition in Australia does not cover all blanket access control measures – a measure must be designed to "prevent or inhibit" copyright infringement in order to attract the protection of the Copyright Act. It was unclear where this left dual purpose measures, such as DVD region controls. However, in the recent *Sony v Stevens* case[1], as well as taking a broad view of what was required to establish that a measure "prevents or inhibits" copyright infringement, the Full Federal Court clarified that so long as a measure serves a copyright protective purpose, the fact that it has another purpose does not take it outside the definition of "technological protection measure". This decision has attracted criticism from the Australian Competition and Consumer Commission and is likely to be a key focus of the Review.

In this area, the Australia-US FTA negotiations will also influence the policy debate, with the US expected to push for bans on both the act of circumvention and the use of circumvention devices and services, to match those in the DMCA.

Corporate libraries

Although not really a "digital" issue, when it was first introduced to Parliament, the Digital Agenda Bill contained a definition of "library" that excluded libraries operated by for-profit organisations, such as corporations and law firms. The effect of the definition would have been to prevent such organisations from relying on the libraries and archives exceptions in the Copyright Act. This was supported by copyright owners, who argued that profit-making organisations should have to pay for their use of copyright material. However, the definition was strongly opposed by user interests, particularly representatives of libraries and educational institutions, who claimed that effectively excluding for-profit libraries from the inter-library loan network would restrict public access to the often highly specialised collections maintained by those libraries.

The Government agreed to remove the definition, but only on the understanding that the issue would be re-considered as part of the Review. The Government has made it clear that it expects the affected interests to provide evidence about the economic impact of the inclusion or exclusion of for-profit libraries from the definition.

[1] *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003)

New anti-"spam" initiatives

Tony O'Malley and Alicia Campos, Mallesons Stephen Jaques

Tony O'Malley is Partner in Mallesons Stephen Jaques' Sydney office and Alicia Campos is solicitor in the Melbourne office. Both work in the Telecommunications Team.

Introduction

On 23 July 2003, the Minister for Communications and Information Technology, Senator Richard Alston, announced the federal government's intention to introduce legislation to ban email "spam". While the legislation will be some time in the making, this announcement marks a timely opportunity to reflect on the current and potential future regulation of marketing through electronic media.

A key point to note is that the current and proposed prohibitions seek to distinguish between unsolicited spam and legitimate marketing activities. In essence, marketing which is requested, consented to or within persons' reasonable expectations or within an existing business relationship should remain permissible. The government has indicated an intention to develop a practical system which permits legitimate marketing but prohibits harassment.

"Spam"

The term "spam" is used for unsolicited electronic marketing or electronic "junk mail" and is readily associated with pornography, scams and black markets. While spam is most frequently used in the context of unwanted advertising e-mail, it is increasingly applied to marketing received via short message service (SMS) and other wireless marketing technologies (such as wireless applied protocol (WAP), multi-media message service (MMS) and third generation technology (3G)).

E-mail spam is still the most prevalent form of spam given its low cost, the ability to include more information in each message and the viability of global internet commerce. However SMS spam is on the rise, particularly with the introduction of bulk discount and web-based SMS generating products. Accordingly, both e-mail spam and SMS spam have attracted recent regulatory attention.

The vice of spam

It is the intrusive nature of spam that arouses concern. Although some traditional forms of paper marketing are dubbed "junk mail", when unwelcome ultimately these materials can be easily disposed of and even recycled. In contrast, electronic spam has been said to threaten the very future of e-mail and SMS as legitimate forms of communication. Electronic spam takes up data usage allowances, which are considerably limited in the case of SMS. Electronic spam is time consuming to delete and invades valuable business hours. Further, there is something intrinsically personal about receiving a message sent to an e-mail address or mobile

phone number – this marketing is more targeted than a random leaflet deposited in a letterbox.

Current regulation

Privacy Act 1988 (Cwth)

The recently introduced National Privacy Principles (NPPs) touch on direct marketing methods. In order for a corporation to use a person's personal information for marketing purposes (eg by e-mail or SMS), that use must be permitted by NPP 2.1. That is:

- the marketing must be one of the primary purposes for which the person's personal information was collected;
- the marketing must be a related secondary purpose of collection and be within the person's reasonable expectations; or
- the person must have given consent (either express or implied) to the use of their personal information for marketing purposes; or
- the person must have been given an opportunity to opt out of the marketing.

Prior to the introduction of the legislation, the Privacy Commissioner published non-binding views that express consent for electronic forms of marketing is preferable.

Australian Communications Industry Forum (ACIF) - SMS Issues Code

The ACIF SMS Issues Code (13 June 2003) is binding on all telecommunications carriers and carriage service providers. This industry specific Code mirrors the Privacy Act provisions above in the specific context of SMS. Additionally, it allows carriers to send "service related messages" and requires carriers to direct organisations with whom it has bulk SMS commercial arrangements to comply with the privacy rules and to terminate those arrangements for non-compliance.

Australian Direct Marketing Association (ADMA) - M-Marketing Code of Practice

The ADMA Code (19 June 2003) is mandatory for all ADMA members. The Code establishes special protections for marketing to children and covers a range of wireless marketing technologies (SMS, MMS, WAP and 3G). Corporations will comply with the Code if message recipients have requested the message, have an established business/contractual relationship or have provided prior consent. A tangential initiative is ADMA's mobile marketing opt-out service which allows consumers to contact ADMA and have their names removed from mobile marketing campaigns.

Proposed email spam legislation

The drafting of the legislation will take place in consultation with industry (particularly Internet Industry Association (IIA) and the Australian Information Industries Association (AIIA)), will be in line with the Privacy Act provisions and enforced by the Australian Communications Authority (ACA). It is contemplated that the legislation will only cover e-mail spam.

The legislation will:

- ban the sending of commercial electronic messages without the prior consent of end-users unless there is "a customer-business relationship" (presently undefined);
- impose a range of penalties for breaking the law including fines, infringement notices and the ability to seek injunctions;
- require all commercial electronic messages to include an opt-out mechanism and the sender's contact details;
- ban the use of e-mail addresses harvesting software; and
- aim to co-operate with overseas organisations to develop international guidelines and mechanisms to battle spam.

Only Australian originated spam will be targeted and businesses will have a 120 day "sunrise period" to bring their practices into line once the new legislation commences.

Senator Alston's Office and the National Office for the Information Economy have proclaimed the steps as world-leading. Legislation in several US States and European Union directives are less ambitious in scope.

Considerations for business

In anticipation of the new legislation and mindful of the current regulatory regime, businesses should:

- obtain advice as to which legislation applies and its implications;
- formulate appropriate marketing strategies, including decisions on implementing opt in/opt out mechanisms;
- give appropriate consideration and implement approvals processes in relation to the frequency, content and relevance of proposed messages; and
- monitor public response to marketing messages sent.

Useful web-sites

Office of the Minister for Communications, Information Technology and the Arts: http://www.richardalston.dcita.gov.au

Department of Communications, Information Technology and the Arts: http://www.dcita.gov.au

Office of the Federal Privacy Commissioner: http://www.privacy.gov.au

National Office for the Information Economy (NOIE): http://www.noie.gov.au

Internet Industry Association (IIA): http://iia.net.au

Internet Industry Association (IIA) - national spam initiative (including e-mail spam filters): http://iia.net.au/nospam

Australian Direct Marketing Association (ADMA): http://www.adma.com.au

Copyright Online: A short note on the proliferation of content distribution technologies online, its implications for the law and suggestions for the future

Abhishek Singh

Abhishek Singh is a final year law student at Sydney University.

Introduction

Barlow once claimed that the Internet would sound the death knell of copyright[1]. However, far from being dead in the online context, recent legislative changes in copyright law[2] seem to have tipped the balance, to an unjustified degree, in favour of the proprietors of copyright content. Bowrey and Rimmer argue that such changes will expand copyright owners' rights beyond the envisioned protective scope of copyright[3]. This article argues that theirs is a more accurate portrayal of the situation than Barlow's now outdated statements. It is then argued that copyright will survive online, but the current situation requires rethinking the level of protection the law should endorse for online content. The article concludes by suggesting that the online content protection that content owners have and are seeking can be appropriately modified. Such actions may, in the online context, go toward striking an appropriate balance between the law permitting hegemonic protection of content, and the law permitting fair use of such content.

Copyright in Physical Space

Copyright law justifies its existence as being the embodiment of the balance[4] between encouraging creativity via the incentive of temporary monopoly profits, and facilitating access to that creativity. In physical space, this balance was struck by allowing fair dealing defences[5], with users free to access and use works so long as their use fitted within one of the fair dealing purposes in the *Copyright Act* 1968 (Cth) (the **"CA"**)[6]. The only protection copyright content had was legal, a porous covering allowing fair users to pass through its regulatory net, and imposing sanctions upon those that sought to unfairly[7] appropriate the profit from the fruit of another's intellectual labor.

This worked because the cost of reproducing and distributing works in physical space is relatively high (e.g. making 100 copies of a book is tedious) and unlawful distribution is generally centralized, therefore easier to trace and regulate.

The Digital Millennium Copyright Act (US) 1998 and Copyright Amendment (Digital Agenda) Act 2000 (Cth): War at the Application Layer for control at the Content Layer[8]

The rise of Napster, and similar phenomena,[9] sparked a legislative reaction in the United States driven by the needs of 'commercial' content producers and distributors.[10] This led to the *Digital Millennium Copyright Act* (US) 1998 (the **"DMCA"**), and a roughly equivalent Australian Act, the *Copyright Amendment (Digital Agenda) Act* (Cth) 2000 (the **"CDA"**), followed. The Australian legislation, as characterized by Oi[11], approved a code based protection[12] on top of the legal protection accorded to copyright content[13], and added another layer of legal protection for the code to the protective package. The crucial point here is this: in the online context, law becomes **both** a source of protection **and** a justifier and endorser of the technology protecting copyright, as opposed to the real world, where copyright law **is** the **only** source of content protection.

Copyright in Cyberspace: Moat and Drawbridge

By allowing code based protection and mandating legally that such code cannot be circumvented, law allowed content owners to build moats around their content, granted them exclusive control of the drawbridge and allowed them to legally challenge those that scaled their walls without permission. Though fair use is incorporated, it is conditioned on permissible circumvention of the code, not independent of it.[14] This is the hindrance to fair dealing in the online context that many complain about.[15] Think of it as law allowing dictatorship at the content layer.

Online Copyright Cases

Traditionally, copyright required an identifiable target to render liable, hence where many procured pirated wares the supplier of those wares was liable and where many infringed copyright due to the direct involvement of another, that other was liable for infringement. This principle is what the courts sought to apply, and applied quite successfully[16], in *A&M Records Inc v Napster*[17] and *Universal City Studios v Corley*[18]. In both those cases, plaintiffs were able to trace liability to a central source directly involved in infringement.

The response then, would be to decentralize infringement, and that is what happened in *MGM v Grokster,*[19] where anonymous, decentralized file sharing technology exposed the limitations in laws premised on physicality and upon the assumption of a source to which infringement could be traced.[20] In *Grokster*, because no substantive source (in the sense of an organization or individual directly enabling infringement as opposed to an end user of the technology) directly involved in infringement was identifiable, liability could not practically be imposed.[21]

Bowrey & Rimmer and Barlow: Realists and Dreamer

Barlow posits a future where creative expression is stripped bare of even the