Copyright and fair use in the digital age

By Louise Longdin

"The whole of human development is derivative. We stand on the shoulders of the scientists, artists and craftsmen who precede us. We borrow and develop what they have done: not necessarily as parasites, but simply as the next generation. It is at the heart of what we know as progress. [B]orrowing and developing have always been acceptable."

– JUSTICE H. LADDIE

Ever since copyright was conferred on authors by the Statute of Anne in 1709 for "the encouragement of learning", one issue in particular has troubled and divided the world's trading nations. This is the problem of how to fairly balance the interests of creators and owners of copyright material against the needs of those who wish to use and build on that material (or maybe even just parody or criticise it). For more than a century, however, an appropriate balance has been struck between people given exclusive rights over works and potential users of those works.

This balance is contrived in two interlocking ways. The first operates through a very important judge-made principle in copyright law (the so-called ideas/expression dichotomy) that fosters the free dissemination of ideas in order to encourage cultural, social and economic development while still protecting the way in which those ideas are expressed. The second is enshrined in Article 9(2) of the Berne Convention 1896 which New Zealand, as a signatory to the World Trade Organisation Agreement on Trade Related Aspects of Intellectual Property Rights, is bound to implement. Article 9(2) sets up a three-step fair

Authors are also increasingly aware that new technologies may infringe their moral rights since it is easy to misattribute or not attribute digital works and subject them to derogatory treatment

use test that permits copying "artistic and literary works in special cases provided that [it] does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author".

Some countries, such as the United Kingdom, Australia, New Zealand and Singapore, try to meet the Berne fair use test by providing for an array of specific statutory exemptions, allowing limited copying for the purposes of private use or study, education, research, archival creation, news reporting, criticism and review. None of these is particularly directed at the use of works in digital networked environments. By contrast, the United States attempts to strike the balance by means of a broad fair use exemption that applies equally to all categories of potential users and uses and thus is more easily adapted to technological and cultural change.

With no bright line drawn between the two ends copyright is made to serve, it has happened from time to time that new communication and information technologies have exacerbated the tension between owners and users. The advent of photocopying in the 1970s led to easy proliferation of copies and necessitated a recasting of international copyright standards to cater for reprographic processes. Now digital communication and information systems have again disrupted the balance between the two groups of stakeholders. Today's hyper-connected world allows all kinds of information (be it text, sound, music, film, graphics or photographic) to be quickly, easily, perfectly and often anonymously copied, transmitted, uploaded, downloaded, manipulated or linked to a site in any jurisdiction. It represents serious danger to copyright owners' interests. Authors are also increasingly aware that new technologies may infringe their moral rights since it is easy to misattribute or not attribute digital works and subject them to derogatory treatment. Conversely, long-accepted fair use rights may be eroded if the law assists owners too assiduously in their attempts to exploit their works using those same technologies.

FAIR USE OF DIGITAL WORKS – ONE STEP FORWARD AND TWO BACK?

It is unavoidable in the digital age that one must often have to first copy the whole of a work in order to fairly use a part of it. Such an action is prima facie copyright infringement. More than a decade ago, however, in the landmark US case Sega v Accolade, the court was prepared to construe as fair use the copying by the defendant of all of a protected computer program to identify a small piece of unprotected code contained within it, required to achieve interoperability between two programs. Accolade had reverse engineered the program Sega used to run a popular video game console to create another independent games platform. The rationale was that if Sega had been allowed to restrict access to technical standards in which copyright did not subsist, it might have inhibited development of an independent and potentially superior games platform.

In the US, Australia and all European Union member states, legislative steps have also been taken to recognise reverse engineering as non-infringing for certain limited purposes such as debugging or making programs interoperable with other independent programs. In contrast, in New Zealand, although the Layout Designs Act 1994 allows reverse engineering of programs for "evaluation and analysis" where those programs are contained in integrated circuits, in all other cases copying to engage in reverse engineering must be squeezed into the "research and private study" exemption which, on the face of it, does not allow copying of the whole of a work in order to use even an insubstantial part. The Ministry of Economic Development (MED), in its Digital Technology and the Copyright Act 1994: Policy Recommendations (presented to the Cabinet Economic Development Committee in June 2003), has suggested the creation of two new exceptions for lawful users of non-infringing programs. One would allow them to decompile software to obtain information necessary to create an independent, but not substantially similar program, where that information is not otherwise

readily available. The other would permit them to copy and adapt programs for error correction or to facilitate interoperability where a functioning or error-free version of the program is not made available within a reasonable time and at a reasonable price.

Even in jurisdictions presently more friendly to users than New Zealand, the recognition (pro users) that reverse engineering for certain purposes may constitute fair use of a work has been increasingly offset by other gains made by copyright owners, gains made on two closely interconnected fronts. The first is owners' recourse to private ordering measures. In seeking new solutions to copyright problems arising out of the use of new technologies, copyright owners have looked to those very same technologies to tip the balance further in their direction. The second victory for owners is their new ability to legally enforce those technological protection measures and prevent interference with digital rights management information systems.

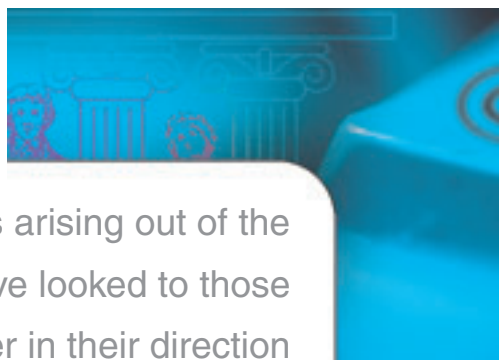
The claimed downside for users is that if digital technology is used to lock in or drip-feed protected copyrighted expression, they may be cut off from facts and formative ideas and deprived of the fair use of works and information that the law would otherwise permit. Users claim this remains their right even in a digital world, begging the question that fair use is by nature a right in itself, not simply a defence to a claim of infringement. Indeed in New Zealand the fair use provisions are called "permitted acts", lending weight to the argument that they are positive rights. This may be crucial in deciding not only whether it is acceptable to allow circumvention of a technological protection measure in order to make fair use of a work (and any public-domain material not subject to copyright fenced in with it), but also whether it is unacceptable to allow copyright owners using click-wrap or browse-wrap licences to erode or do away with public ordering mechanisms such as fair use in their generally non-negotiable terms and conditions.

The legitimate as well as the self-serving arguments and private ordering mechanisms used by owners are explored in what follows in the light of various recent legislative enactments in the US, the European Union and Australia and bearing in mind the review the New Zealand government is conducting of its copyright legislation in relation to digital technology. The government has instigated the review largely in order to position itself to comply with the two 1996 World Intellectual Property Organisation (WIPO) "Internet Treaties" to which it plans to accede, namely the WIPO Copyright Treaty (WCT) and the WIPO Performers and Phonograms Treaty (WPPT). It is suggested that when new copyright standards are implemented by New Zealand, they should be carefully crafted to avoid as far as possible any distorting flow-on effect on the traditional international copyright standard of fair use. It is reassuring that MED's recommendations state that the review intends to ensure that the balance between protection and incentives for copyright owners and access to users remains in the digital environment.

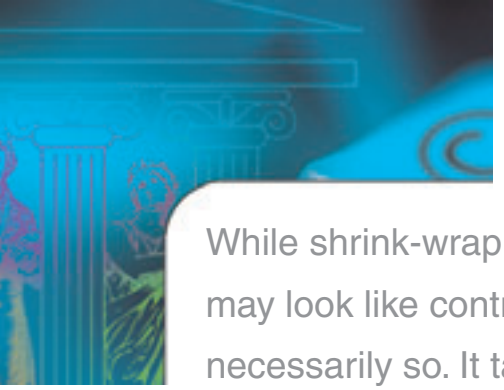
TECHNOLOGICAL MANAGEMENT OF ACCESS TO AND USE OF DIGITAL WORKS

Various kinds of digital rights management systems (DRMS) have been developed by owners of electronic copyright works and information products to achieve one or more of the following ends:

- To prevent unauthorised initial access to their works or products (no browsing).
- To meter access to their works or products (pay-as-you-view business models).



In seeking new solutions to copyright problems arising out of the use of new technologies, copyright owners have looked to those very same technologies to tip the balance further in their direction



While shrink-wrap and click-wrap licences may look like contracts, they are not necessarily so. It takes two to contract

- To identify themselves as the owners and/or authors of those works or products.
- To set out terms and conditions of access or use and ensure access/use occurs only in line with such terms and conditions.
- To register and then verify user identification details.
- To track online consumption patterns of protected material by individual users and product tampering.
- To track dissemination of material to a particular computer terminal, if not to the actual user.

The general term DRMS is thus used here to embrace both technological protection measures (TPMs) and digital rights management information systems (DRMIS). As foreshadowed above, concern is mounting that owners are resorting to TPMs to restrict copying of and access to works even (or perhaps especially) when that use would be permitted on ordinary fair use principles. Probably the best-known (certainly much-litigated) example of a TPM is the content scramble system (CSS) used by movie studios to stagger the release of their movies on DVDs to eight regions in the world. CSS controls access to the sound and graphic files contained on those DVDs via a dual-key encryption system. Encrypted files on a DVD are decrypted by an algorithm stored on both the DVD itself and the DVD player or any other authorised platform such as Macintosh and Windows operating systems. CSS is intended by owners to prevent the content of their DVDs being played on open-source platforms such as LINUX.

In tandem with TPMs, owners have resorted to shrink-wrap, click-wrap and browse-wrap licences to set out DRMI in relation to the work in question, identifying the owner of the work and again providing for terms and conditions of access and/or use. Click-wrap and browse-wrap licences evolved from shrink-wrap licences (so called because many software developers distributed their products to users on standardised terms contained on disks inside plastic-encased boxes). Click-wrap and browse-wrap licences cater for software delivered electronically to users, allowing them to access and/or use the product only after clicking one or more screen icons saying “I Accept, “I Agree” and such like. Browse-wrap licences, as their name suggests, allow users to view terms and conditions via one or more hyperlinks. The attraction of such delivery mechanisms for owners is due to the notion that they allow them to “licence” rather than “sell” their electronic products. Otherwise the first-sale rule would mean they enjoyed no rights over the tangible copies of their works after sale and thus could not prevent first users from disposing of their computers or master disks with the works installed on them to second users, and second users in turn to third users, and so on.

While shrink-wrap and click-wrap licences may look like contracts, they are not necessarily so. It takes two to contract. The question of their enforceability depends largely on the law of offer and acceptance (fairly uniform across most common law jurisdictions) and has been decided so far on a case-by-case basis. The issue was first decided affirmatively in 1996 in the US in ProCD Inc v Zeidenberg. The computer-scientist purchaser of a $US10-million database on CD-ROM had separated out the unprotected facts in the database (telephone numbers) from the search engine (a protected computer program), then written and substituted his own search engine program and offered the “new” database for sale on the internet. He was found on appeal to have infringed the terms and conditions of the shrink-wrap licence that physically came with the software and clearly stipulated that the database was not to be copied for commercial purposes.

It was a pivotal factor in the case that the purchaser had the opportunity to read and reject the conditions and obtain a full refund. Other US cases, notably Groff v AOL (1998) and Hotmail Corp v Van Money Pie Inc (1998), have subsequently found click-wrap and browser-wrap licences to be valid and enforceable. That said, end-user licencing agreements (EULAs) in

electronic form will still have to be installed for end users to have the opportunity of reading them and agreeing to be bound. This was the finding in the Scottish and US cases Beta Computers v Adobe Systems (1996) and Softman Products v Adobe respectively. In Adobe, a software manufacturer had distributed copies of four of its products as a package (Adobe Pagemaker, Acrobat, Photoshop and Illustrator). The defendant purchased copies of the package from an authorised distributor and sold the applications separately from its website www.buycheapsoftware.com for less than Adobe did. The collection was distributed with a EULA expressly prohibiting unbundling the collection for resale. The EULA said that if users transferred the collection, they had to transfer the software as an entity. Adobe was not in any contractual relationship with Softman, but still claimed Softman was bound by the EULA. Softman contended, however, that after the first sale of the collection, Adobe had no say over what Softman did with the tangible physical copies as long as it did not copy the master to make copies for sale; that Softman could give them away or sell them separately as indeed it did.

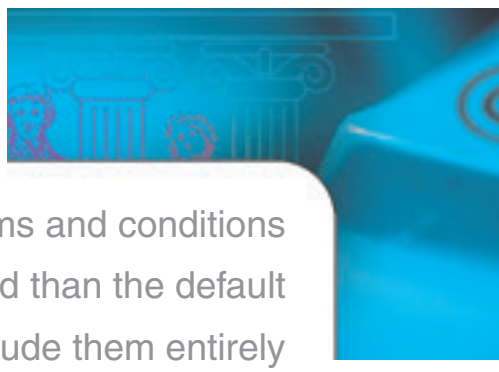
In determining whether Adobe's EULA bound Softman, the court noted that the EULA's terms and conditions were not displayed on the outside of the package nor were they affixed to any of the application disks inside. The EULA was displayed only when a user inserted any one of the four disks containing the application into a computer. The program would not install itself on the user's hard drive unless the user agreed to accept the conditions. Since Softman did not install any of the applications before resale, it was found not to be bound.

In another US decision, Specht v Netscape Communications Corp (2001), it was also found necessary that end users have the opportunity to review terms and conditions before they agree to a browse-wrap licencing agreement. In that case, Netscape could not enforce its EULA after offering SmartDownload software on the internet because its terms and conditions were not available on the download page, but only via a series of hyperlinks. Any user could thus obtain (and presumably make fair use of) the program under copyright law.

When EULAs are enforceable, however, they may provide terms and conditions of access and/or use of works that are more limited than the default statutory fair use exemptions and may even exclude them entirely. For example, many jurisdictions including those of the US, European Union member states, Australia and New Zealand allow licenced users to make a back-up copy of a computer program. A EULA may deprive the user of that statutory right.

ANTI-CIRCUMVENTION SANCTIONS

Copyright owners have argued strenuously that their DRMSs must be able to be enforced effectively against thieves and pirates. As one commentator, Dusollier, explained their perceived plight: "[For owners] building a technical fence around works [was not] sufficient. Electrifying it by making its circumvention a criminal act was needed." The backlash reaction by users to owners' lobbying for wider rights over their works resulted in the US in what another commentator, Forsyth, aptly described as "a mighty battle between Hollywood and Silicon Valley". Hollywood sought to have outlawed actual circumvention of TPMs, the manufacture, importation and distribution of circumvention devices and even dissemination of information about circumvention techniques. Silicon Valley, for its part, sought to carry on engaging in lawful reverse engineering, computer security testing and encryption research.



When EULAs are enforceable, they may provide terms and conditions of access and/or use of works that are more limited than the default statutory fair use exemptions and may even exclude them entirely

The crux of the offence lies in bypassing the lock, with penalties commensurate with the degree to which the access has been for commercial advantage or commercial gain

Non-technical copyright users also objected that allowing owners to control access to and use of works flies in the face of the time-honoured practice of browsing in the analogue world where users are free to browse through works and to copy part (if not a substantial part) for private research and study purposes. Users also protest that TPMs may be used to lock up information in the public domain, information that should be available to all. Why, they ask, should they have to pay for access or even have to go through the motions of negotiating access to public-domain material with those who use TPMs to lock it up?

Strong lobbying for greater anti-piracy measures largely from US copyright holders (the US being the world's largest exporter of copyright material) led to new rights for copyright owners being laid down in the two 1996 WIPO treaties now part of the law in the 41 countries that have to date ratified them. Article 11 of WCT requires states to enact "adequate legal protection and effective legal remedies against the circumvention of effective technological protection *measures* that are used by authors under [WCT or Berne] and that restrict acts, in respect of their works, which are not authorised by the authors concerned or *permitted by law*". (This last phrase is an oblique reference to fair use exemptions under either statute or case law.)

Article 12 of WCT requires states to enact adequate legal protection and effective legal measures against people who alter or remove "rights management information" (RMI) without authority. RMI is information "attached to a work or appearing in connection with the communication of a work to the public which identifies the author and sets out the terms and conditions of its use". Article 12 also covers people who knowingly import, distribute, broadcast or communicate to the public without authority copies of works with RMI altered or removed. In neither article are the terms "adequate" and "effective" defined. As to fair use limitations that may be imposed on owners' rights, Article 10 of WCT essentially affirms the Berne three-step fair use test. Interestingly, there is also an Agreed Statement attached to Article 10 that states *may* carry over and extend fair use exceptions devised for the analogue world to the digital environment. The Agreed Statement also says that new fair use provisions *may* be devised. (However, even had the Agreed Statement said *must* instead of *may*, countries ratifying WIPO treaties are not in any event required to implement Agreed Statements that are used to signal a strong reservation or message on the part of some, but not all, countries taking part in the diplomatic conference framing the treaty in question.)

LEGISLATIVE RESPONSES TO THE WCT IN KEY JURISDICTIONS

Not surprisingly, the US was one of the first countries to respond to the WCT by enacting its Digital Millennium Copyright Act 1998 (DMCA). As well as civil sanctions, it creates heavy criminal sanctions (five to 10 years' imprisonment and fines up to $US1 million) for wilful circumvention. The legislation relies heavily on the metaphor of a locked house. First, it seeks to allow owners to control access to copyrighted works (rather like stopping someone from actually breaking into a locked house to obtain a copy of a work). Secondly, it aims to stop trafficking in anti-circumvention tools or technology primarily designed to enable breaking into locked houses that contain a work.

There are mirror provisions in relation to anti-copying devices and technology. The prohibition against actual circumvention holds, even if access gained through circumvention does not lead to an infringement of copyright – for example, if only public domain material is taken. The crux of the offence lies in bypassing the lock, with penalties commensurate with the degree to which the access has been for commercial advantage or commercial gain. Similarly, liability may be imposed for distribution of a circumvention device for copying, even if the resulting end use is lawful.

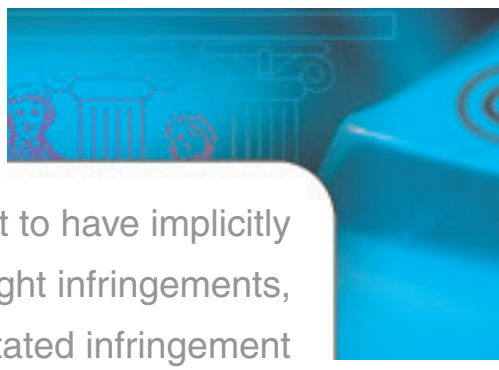
At first blush, the DMCA does not limit fair use since Section 1201(c)(1) states encouragingly that

"nothing in this section shall affect … limitations, or defences to copyright infringement, including fair use". This is cold comfort for users, however, because unless they are able to gain authorised access to works, they cannot make fair use of them. The DMCA also contains certain specific exceptions for law enforcement and other governmental agencies; non-profit libraries, archives and educational institutions, solely to determine whether they wish to obtain authorised access to works; reverse engineering solely to achieve interoperability; encryption research and security testing; and the protection of privacy and minors.

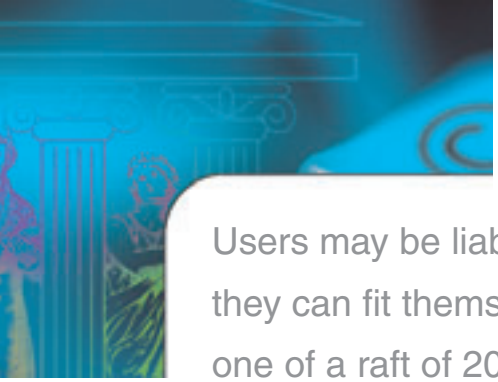
It appears after the US case Realnetworks Inc v Streambox Inc (2000) that one of the most far-reaching effects of the DMCA is that owners can now sue a small number of easily identifiable, deep-pocketed distributors within their own jurisdiction rather than a mass of potentially infringing individual users who could be anywhere. In Realnetworks, the plaintiff won an interim injunction to restrain Streambox from distributing its product Ripper, designed to decode audio and visual files intended to be played on Realplayer. Since the device was designed for one purpose only, to decode, the decision can be distinguished from the landmark case Sony Corp of America v Universal City Studios (1984) in which the US Supreme Court found copyright is not infringed merely because someone sells a device that is capable of being used for copying if the device is also capable of non-infringing use, too. The decision in 1988 by the House of Lords in CBS Songs Ltd v Amstrad plc was in similar vein and based on UK legislation close to that later adopted by New Zealand in its 1994 copyright legislation. In the latter case, manufacturers of double-headed audiotape decks were found not to have implicitly authorised their customers' copyright infringements, despite the fact that their product facilitated infringement and they knew infringement was likely to occur. The pivotal factors were that the means to infringe could be used for perfectly legitimate as well as infringing purposes and the suppliers had explicitly warned users against copyright infringement.

Much of the post-DMCA litigation to date has focused on attempts to protect the CSS measure, however, although it was only a weak 40-bit encryption system and was successfully hacked in 1999 by an anonymous German. After a de-encryptor device, DeCSS, was developed to allow DVDs to be played on any platform and their contents uploaded on to the worldwide web, an action was brought against a Norwegian who first put DeCSS online. Since he was a hard target being not only young (15), but out of the US jurisdiction at the operative time, litigation shifted successfully closer to home in Universal Studios Inc v Reimerdes to a person who had uploaded DeCSS from several US-based websites. Buttressed by the outcome of this case, copyright owners threatened action against people with printed T-shirts proclaiming the DeCSS code as well as actually suing those referring to it in anecdotal stories, as in Universal City Studios v Corley (2001). In that case, the defendant Goldstein (using the pseudonym Corley) wrote and put online a story about the reverse engineering of CSS, the creation of DeCSS, the Norwegian boy's plight and, most damningly, included a link on his website to DeCSS. As the court said, this was akin to publishing the combination to a bank vault.

Strictly speaking, the DMCA prevents any person publishing information that may lead to circumvention of a TPM. That this stricture may make it difficult for computer scientists and academics in the US to publish their research for career advancement is well illustrated by the dilemma facing a Princeton professor and computer



Manufacturers were found not to have implicitly authorised their customers' copyright infringements, despite the fact that their product facilitated infringement



Users may be liable for infringement unless they can fit themselves under the umbrella of one of a raft of 20 or so narrow exemptions

scientist in Felten v Recording Industry of America. In 2001, Felton wanted to publish a scientific paper explaining how he had overcome TPMs developed by the Secure Musical Initiative (SMI) and, quite wisely, sought a declaration from the court that he would not be infringing the DMCA by doing so. But the court dismissed the action on the ground that there was no actual case or controversy. While not articulating the reasons for the dismissal very clearly, the court seemed to be influenced by the plaintiff's primary purpose, which was to assist the strengthening rather than the circumvention of access controls.

The European response to the WCT lies in its 2001 Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society that was required to be implemented by all member states by December 22, 2002. It adheres to the US model fairly closely in that it expands owners' rights by prohibiting both acts of circumvention and circumvention devices. Article 6 requires that: "Member states shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective." The provision further requires member states "to provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement or possession for commercial purposes of devices, products or components or the provision of services that: are promoted, advertised or marketed for the purpose of circumvention, or have only a *limited commercially significant purpose or use other than to circumvent*, or are primarily, designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures".

The Directive contains no exemption for research or private study, criticism or news reporting. Users may be liable for infringement unless they can fit themselves under the umbrella of one of a raft of 20 or so narrow exemptions all bar one of them purely voluntary rather than mandatory for member states to implement into their national legislation. The exemptions include: specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage; use for the sole purpose of illustration for teaching or scientific research; use for the benefit of people with a disability and use for the purpose of public security or for reporting administrative, parliamentary or judicial proceedings. This list does not even pay lip service to the Agreed Statement to Article 10 (which, as already mentioned, suggests states may make accommodation for fair use in the digital environment). To further undermine the position of potential fair users, Article 6 IV of the Directive requires that users must already have legal access to the protected work in question in order to be assisted by the owner in exercising their right of fair use.

The Australian approach to implementing WCT is relatively benign to both users and equipment manufacturers and distributors. Actual use of a circumvention device or service is not prohibited under the Copyright Amendment (Digital Agenda) Act 2000 (CADA) and a "circumvention device", while it is defined to include a computer program, excludes general-purpose equipment such as CD burners, video or tape recorders and computers. Interestingly, there is a different burden of proof requirement depending on whether civil or criminal proceedings are involved. For criminal liability (carrying imprisonment of up to five years and hefty fines), the prosecution must prove actual knowledge or recklessness. In a civil action, the onus shifts to defendants to prove they did not know or ought not reasonably to have known that a particular circumvention device or service would be used to circumvent. While no fair dealing exception exists, some narrow exceptions exist including the ability to reproduce computer programs to make interoperable products, to correct errors and for security testing and law enforcement. To rely on one of the exceptions, however, it is necessary to

sign a declaration that the device will be used only for the permitted purpose.

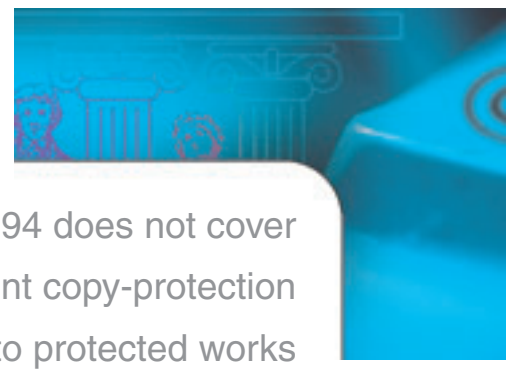
Australia has already experienced teething problems with CADA and in April 2003 amended its requirement that a circumvention device be capable of circumventing or facilitating the circumvention of an "effective" TPM. It removed the word "effective" from the definition of "circumvention device" after the Federal Court in Kabushiki Kaisha Sony Computer Entertainment v Stevens found in favour of the defendant who had supplied and installed a "Mod Chip" in Sony PlayStation consoles so that games unlawfully copied on to CD-ROM could be played on them without the non-reproducible access code by which the boot ROM device housed in the consoles recognises lawful copies of the games. The Federal Court judge decided that a TPM must be designed to prevent or inhibit post-access infringement of copyright and that the Sony mechanism only deterred or discouraged copyright infringement in the computer games. It did not, he found, physically prevent or inhibit infringement by copying games on to CD-ROM. The amendment (unusually) was given full retrospective effect back to 2002 when CADA was passed. When it fell to the full Federal Court to decide Kabushiki on appeal in July 2003, all three judges preferred the broader construction of the TPM definition, finding against the defendant on the ground that the Sony device to be circumvented by the Mod Chip was a TPM. Thus, the situation in Australia post-Kabushiki is that it is legal to own and use a Mod Chip, but illegal to sell them.

THE OPTIONS FOR NEW ZEALAND

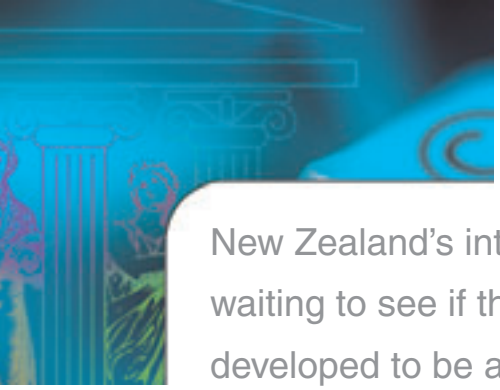
At present, Section 226 of the Copyright Act 1994 prohibits providing the means or information or a device to circumvent copy-protection measures by means of selling, advertising, hiring or publishing a decryption code. It requires defendants to know or have reason to believe that the device, means or information will be used to make infringing copies, but does not cover people who actually circumvent copy-protection measures and gain unauthorised access to protected works or people who alter or remove DRMI. The largely similar UK counterpart of this section was successfully invoked in Sony Entertainment v Paul Owen (2002) to counteract the bypassing of Sony's circumvention device in PlayStation2 by means of the "Messiah" chip imported from Russia. The special codes put in the games console by Sony were designed to prevent any of its out-of-zone games from being played (no matter that they might be legitimate copies) as well as unauthorised copies.

While MED, in its Policy Recommendations, proposes that Section 226 be strengthened to allow copyright owners to take action when any of their exclusive rights are infringed not just by copying, it also warns that allowing TPMS to prevent the playing of non-pirated copies of games from zones where there is no copyright infringement may fall foul of our current parallel importing regime.

As it contemplates implementing the 1996 WIPO Treaties, New Zealand faces a choice, a choice that involves compromise, not a crude bipolar decision that the greater harm lies in allowing either (i) users to overstep their rights of fair use to the extent of commercially exploiting copyright material themselves or (ii) owners to enforce private ordering mechanisms to the extent that owners erode or quash altogether the fundamental right of access to information and ideas. It is a choice that must reflect New Zealand's economic position as a net importer of digital works. Why should this country automatically protect access control technology that



Section 226 of the Copyright Act 1994 does not cover people who actually circumvent copy-protection measures and gain unauthorised access to protected works



New Zealand's interests may well be served by waiting to see if the technology can be developed to be as friendly to users as owners

may be used by overseas copyright owners for price discrimination purposes and to delay New Zealand's exposure to cultural products such as DVDs? Price discrimination may be economically efficient in some circumstances, but there is no evidence that efficiency is enhanced by allowing the legislature to chose those circumstances and set them in legislative concrete. This is especially important in a country where intellectual property dealings are for the most part immune from competition scrutiny.

New Zealand's interests may well be served by waiting to see if the technology can be developed to be as friendly to users as owners, distinguishing and accommodating users seeking access to works in order to make fair use of them, as opposed to people bent simply on copying and exploiting them. Even doing nothing may be better than rushing to adopt the anti-circumvention measures (ill considered and much criticised on their home ground) of the US and the EU. We should certainly contrive to end up with nothing more restrictive than the Australian position given the by now almost complete integration of the two economies.

REFERENCES

Bell, T. (1998). Fair Use vs Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine, 76 *NCL Rev* 557.

Dusollier, S. (1999). Electrifying the Fence: Legal Protection of Technological Measures for Protecting Copyright, *European Intellectual Property Review* 285.

Forsyth, M. (2001). The Digital Agenda Anti-circumvention Provisions: A Threat to Fair Use in Cyberspace. *Australian Intellectual Property Journal* 82.

Grosheide, F.W. (2000). Copyright Law from a User's Perspective: Access Rights for Users, *European Intellectual Property Review.*

Heide, T. (2001). Copyright in the EU and United States: What "Access Right"? *European Intellectual Property Review* 469.

Laddie, Justice H. (1996). Copyright: Over-Strength, Over-Regulated, Over-Rated? *European Intellectual Property Review* 259.

Ministry of Economic Development documents at http://www.med.govt.nz

Digital Technology and the Copyright Act 1994, A Discussion Paper (July 2001).

Summary of Submissions Received on the Digital Technology Discussion Paper (July 2002).

Digital Technology and the Copyright Act 1994: Policy Recommendations, presented to the Cabinet Economic Development Committee in June 2003.

European Directive on the Harmonization of Certain Aspects of Intellectual Property and Related Rights in the Information Society (2001).

CBS Songs v Amstrad Consumer Electronic Plc (1988), AC 1013 (HL).

Felten v Recording Studios (2nd Cir 2001), 273 F 3d.

Kabushiki Kaisha Sony Computer Entertainment v Stevens (2003), FCAFC 157.

ProCD Inc v Zeidenberg (7th Circ 1996), 86 F 3d 1447.

Sega Enterprises Ltd v Accolade Inc (9th Cir 1992), 977 F 2d 1510.

Softman Products v Adobe (2001), 171 F Supp 2d 1075.

Sony Corp of America v Universal City Studios (1984), 464 US 417.

Sony Entertainment v Paul Owen (2002), EWHC 45.

Realnetworks Inc v Streambox Inc (WD Wash 2000), 200 WL 127311.

Universal Studios Inc v Reimerdes (2000), 111 F Supp 2d 294.

Louise Longdin

SENIOR LECTURER

The University of Auckland Business School

Email: l.longdin@auckland.ac.nz