IP, PHONE HOME: THE UNEASY RELATIONSHIP BETWEEN COPYRIGHT AND PRIVACY, ILLUSTRATED IN THE LAWS OF HONG KONG AND AUSTRALIA

■

Graham Greenleaf[*]

The development of content-protection technologies (CPT) and digital rights management systems (DRMS), despite their benefits to rights-holders, pose many dangers to the protection of privacy, which some have said could mean an end to the privacy of reading. Hong Kong and Australia are two of the earliest jurisdictions in the world with laws implementing the anti-circumvention and rights management information (RMI) protection provisions arising from the WIPO Copyright Treaty 1996 (WCT). They are also two of the few jurisdictions outside Europe with privacy (data protection) laws applying to the private sector. These two jurisdictions, therefore, give two of the best illustrations of the tensions now arising between copyright and privacy: property versus privacy. In this article, the author explores how CPT and DRMS affect privacy, how existing data protection and privacy laws affect the operation of CPT and DRMS, and whether laws against copyright circumvention devices and interference with RMI prevent privacy protection. The author concludes that privacy could now be unduly prejudiced in favour of property, and suggests reforms which may help restore the balance.

Property Versus Privacy

"Information wants to be free"[1] is one of the "myths of digital libertarianism"[2] that formed the ideology of the pre-commercial Internet. Digital

[*] Distinguished Visiting Professor, University of Hong Kong, Faculty of Law; Professor of Law, University of New South Wales, Australia; Co-Director, Baker & McKenzie Cyberspace Law and Policy Centre, UNSW; g.greenleaf@hku.hk. The first three parts of this paper are based on an earlier version presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13–15 Sept 1999. Thanks to Lee Bygrave, John McPhail, Kevin Pun, Anne Flahvin, Peter Cheung and to the anonymous reviewer of this article for their helpful comments. Responsibility for opinions, conclusions and errors remains mine. Thanks to Janie Wong for editorial assistance. Internet addresses in the references were last checked on 4 Mar 2002 unless stated otherwise.

[1] Almost always attributed (without any source) to Stewart Brand, Electronic Frontier Foundation Board member, and founder of the Whole Earth Catalog and the WELL. *See* below concerning the full quote.

[2] *See* Part II of Graham Greenleaf, "An Endnote on Regulating Cyberspace: Architecture vs Law?" (1998) 21(20) *University of New South Wales Law Journal*, "Electronic Commerce: Legal Issues For The Information Age", http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/greenleaf.html.

libertarians expected intellectual property (IP) law to be one of the first casualties of cyberspace, because the process of digitisation of works made them infinitely reproducible at virtually no marginal cost and infinitely distributable via the Internet. The Internet and property in information were widely believed to be incompatible: technology would win against law and set information free. "Everything [you know] about intellectual property is wrong" claimed John Perry Barlow.[3]

The reverse process is now underway: technical protection of IP in cyberspace (ie over networks) may protect property interests in digital works[4] more comprehensively than has ever been possible in physical space, and destroy many public interest elements in IP law in the process. In the worst scenarios, the surveillance mechanisms being developed to do this may also bring about the end of the anonymity of reading. Privacy is one of the interests threatened.

In criticising Barlow, Lessig observed that infinite copies could only be made if "the code permits such copying", and questioned why the code (software and other aspects of the technical architecture of cyberspace) could not be changed to make such copying impossible.[5] For IP, this architecture involves content-protecting technologies (CPT)[6] and digital rights management systems (DRMS).[7] IP has become one of the areas where cyberspace architecture is said to be replacing law as the most effective method of protecting interests. However, the new adjuncts to IP law discussed in this paper (laws against circumvention devices and laws protecting rights management information (RMI)) are part of this change. Contract law is also a vital part of the new paradigm for protection of digital content. The process is one of law being partly replaced by technology, but with new and different forms of law supporting the protection by technology and vice-versa.

DRMS and CPT have many legal implications, but this paper only focuses on their effect on privacy and their relationship to privacy laws. It explores what protections are found in information privacy laws against surveillance by digital works, their interaction with these new adjuncts to IP laws, and the extent to which privacy laws may need to be strengthened to help provide a reasonable balance between privacy and the protection of IP.

[3] John Perry Barlow, "Selling Wine Without Bottles: The Economy of Mind on the Global Net" *Wired Archive* 2.03 (1993) at 86, http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html.

[4] "Digital works" is used loosely in this article to refer to any digital artefact that could embody copyright subedit matter.

[5] "Code Replacing Law: Intellectual Property" in Lawrence Lessig, "The Law Of The Horse: What Cyberlaw Might Teach" (1998) 113 *Harvard Law Review* 501, http://lessig.org/content/articles/works/finalhls.pdf or http://www.swiss.ai.mit.edu/classes/6.805/articles/lessig-horse.pdf.

[6] There is no widely accepted terminology for individual technologies that protect digital content. The author uses "CPT" to refer to "content protecting technologies" rather than "copyright-protecting", because they protect content which copyright does not protect.

[7] DRMS were also known as electronic copyright management systems (ECMS), but DRMS is the more current terminology.

These tensions between property and privacy are illustrated by the laws of Hong Kong and Australia, because they are two of the earliest jurisdictions in the world to implement the anti-circumvention and RMI protection provisions arising from the WIPO Copyright Treaty 1996 (WCT), and because they are also two of the few jurisdictions outside Europe with privacy (data protection) laws applying to their private sectors. Their laws illustrate the tensions now arising between copyright protection and the protection of privacy: property versus privacy.

Perhaps we have only received a fragment of Brand's[8] aphorism: is it really "Information wants to be free ... but it wants to keep *you* under surveillance"?

Anonymity and Privacy – Traditional IP Rights

We should start by considering some of the ways in which IP laws and enforcement practices have traditionally respected privacy, so as to appreciate better what changes are inherent in new laws and practices. Here are some common, though not universal, features of how users[9] of copyright artefacts experienced copyright law in the pre-digital era (and still do in relation to non-digital embodiments of works):

1 Most sales of artefacts embodying copyright works (books, CDs, videos, etc) were anonymous because they were cash transactions, with payment by identified means at the option of the purchaser, not the copyright owner.

2 Users of copyright artefacts did not usually enter into any contractual relationship with the owner of the copyright, as they dealt only with intermediaries (booksellers, record stores, libraries, etc). This is one reason why copyright was needed as a property right, since contract was inadequate protection for the copyright owner.

3 The artefacts had no inherent surveillance capacities. They would not record (much less, communicate) who had used them, when or where.

4 Copyright law did not give copyright owners a general right to control uses of artefacts embodying their works, other than the specified

[8] One list of famous quotes adds "Among others. No telling who really said this first", http://world.std.com/~tob/quotes.htm. However, John Perry Barlow insists (though he still doesn't give a source) that the full version of Brand's quote is: "Information wants to be free – because it is now so easy to copy and distribute casually – and information wants to be expensive – because in an Information Age, nothing is so valuable as the right information at the right time." (Barlow, in an Atlantic Monthly Roundtable, http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm). The author will adhere to his own imaginary version.

[9] The following description was largely true in relation to the end-users of copyright artefacts, consumers, but was less true of various categories of intermediaries who licensed the uses of copyright works.

"infringing uses" which involved "copying" and a limited number of forms of communication. Consequently, who *read* a book (or watched a film), how often, when and where was generally none of the author's business.

5 Loans of copyright artefacts to others to use were generally beyond the control or knowledge of copyright owners. Where intermediaries such as libraries or video rental stores did keep records of borrowings, these could result in privacy invasions, but usually not by or for the copyright owners.

6 Enforcement of copyright – detection of and action against infringing uses – was therefore not a by-product of routine surveillance of all uses of copyright works, but usually a matter of selective surveillance and periodic detection (*ex post facto*). Enforcement in "real time" (simultaneous with attempted infringement) was generally impossible.

7 There were various types of "fair use" of copyright artefacts (uses which would normally constitute infringements but under certain conditions did not) which did not require the user to seek any licence from the copyright owner or even communicate to the copyright owner that the use was taking place. "Fair use" could also be private use.

8 Some types of infringement would only occur where the act concerned was "in public" (or some similar formulation), effectively creating various types of "private spheres" outside the scope of copyright laws.[10] Although these exceptions to copyright for "private use" are the most obvious form in which copyright law accommodated privacy, it is a mistake to exaggerate their importance.[11] In comparison, the default condition of anonymity in the normal use of copyright artefacts is more important.

Over centuries, a balance was formed between the interests of copyright owners to be aware of infringements and the ability of users to experience intellectual works in private. A traditional right to enjoy works in private resulted. Being able to read or view works free from surveillance is an important support for freedom of conscience, freedom of expression and a democratic society.[12] The new technological protections of copyright are altering this balance.

[10] *See* Lee Bygrave and Kamiel Koelman, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems*, (report commissioned for the Imprimatur project) (Institute for Information Law, University of Amsterdam, June 1998), http://folk.uio.no/lee/articles/ECMS_Imprimatur.pdf; *see* also their chapter in Hugenholtz (ed), *Copyright and Electronic Commerce* (Deventer: Kluwer, 2000) for examples.

[11] *Ibid.*, Ch 5 stresses this reason, giving too little weight to the factors mentioned earlier.

[12] As Bygrave notes in Lee Bygrave, "The technologisation of copyright: Implications for privacy and related interests" (2002) 24(2) *European Intellectual Property Review* 51, part of the function of privacy laws is to protect "the incentive to participate in a democratic, pluralist society by securing the privacy, autonomy and integrity of individuals".

It is possible to argue[13] from an economic analysis of copyright law that such limitations on exploitation of copyright as those outlined above that support respect for privacy are merely a result of previously high transaction costs which DRMS can eliminate. However, they can also be seen as a means of reconciling the loss to the public welfare caused by the monopoly involved in copyright. At least because there is not yet "any well-functioning competition between different DRM systems", and for other reasons, many argue that the law has to limit the extent of protection that DRMS can provide.[14] The author of this article agrees, and takes the same approach to the need for law to balance protection of privacy against the protection of digital content.

Technologies and Systems for Copyright Protection

Pervasive Networking of Digital Artefacts

Kevin Kelly[15] thought that:

> "the trajectory is clear. We are connecting all to everything.
>
> ...
>
> As we implant a billion specks of our thought into everything we make, we are also connecting them up. Stationary objects are wired together. The nonstationary rest – that is, most manufactured objects – will be linked by infrared and radio, creating a wireless web vastly larger than the wired web. It is not necessary that each connected object transmit much data. A tiny chip plastered inside a water tank on an Australian ranch transmits only the telegraphic message of whether it is full or not. A chip on the horn of each steer beams out his pure location, nothing more: 'I'm here, I'm here.' The chip in the gate at the end of the road communicates only when it was last opened: 'Tuesday.'"

Pervasive networking enables a trend toward artefacts that report back through these digital networks to some central monitoring point about their location, current state or prior usage, often in a way which allows that information to be correlated, more or less reliably, with the actions of individual people. Artefacts are often built with surveillance capacities enabled in default, sometimes with an "opt out" capability.

[13] The summary of these arguments on which this is based are from part 6.1.1 of Stefan Bechtold, "From Copyright to Information Law – Implications of Digital Rights Management", *Workshop on Security and Privacy in Digital Rights Management 2001* (Philadelphia, USA, 5 Nov 2001), http://www.star-lab.com/sander/spdrm/papers/bechtold.pdf.

[14] *Ibid.*, the conclusion reached by Bechtold.

[15] Kevin Kelly, "New Rules for the New Economy" *Wired Archive* 5.09, Sept 1997, http://www.wired.com/wired/5.09/newrules.html.

To see that many digital artefacts do live in a networked world is simple enough. Many people now have Internet connections active whenever they are using their computers. Every program, document or other file on their computer is then (in theory) capable of communicating with anywhere else on the Internet, such as the computer system of its copyright owner or of an intermediary in a DRMS. Furthermore, many digital artefacts have their full utility only when their users are online. An obvious example is that word processing documents are now created routinely with live hypertext links, so that the document is interactive if opened when the user's personal computer (PC) is online, but not otherwise. Another example is software for playing recorded music which, when a music compact disc (CD) is inserted in a PC, automatically checks an Internet database to obtain the title and other details of all the tracks on the CD.[16] The telecommunications infrastructure for digital artefacts to exercise surveillance is, therefore, an increasingly pervasive part of our computer use.

Many hardware devices used to present digital content are not yet networked (at least not so as to allow two-way communication), including most CD and digital video disc (DVD) players, and televisions. However, the range of hardware devices used for presenting content with wired or wireless communications capacities is growing rapidly, including mobile phones and personal digital assistants (PDAs). This article concentrates on digital content which is already part of the increasing pervasive networking, because that is where the privacy issues are most acute.

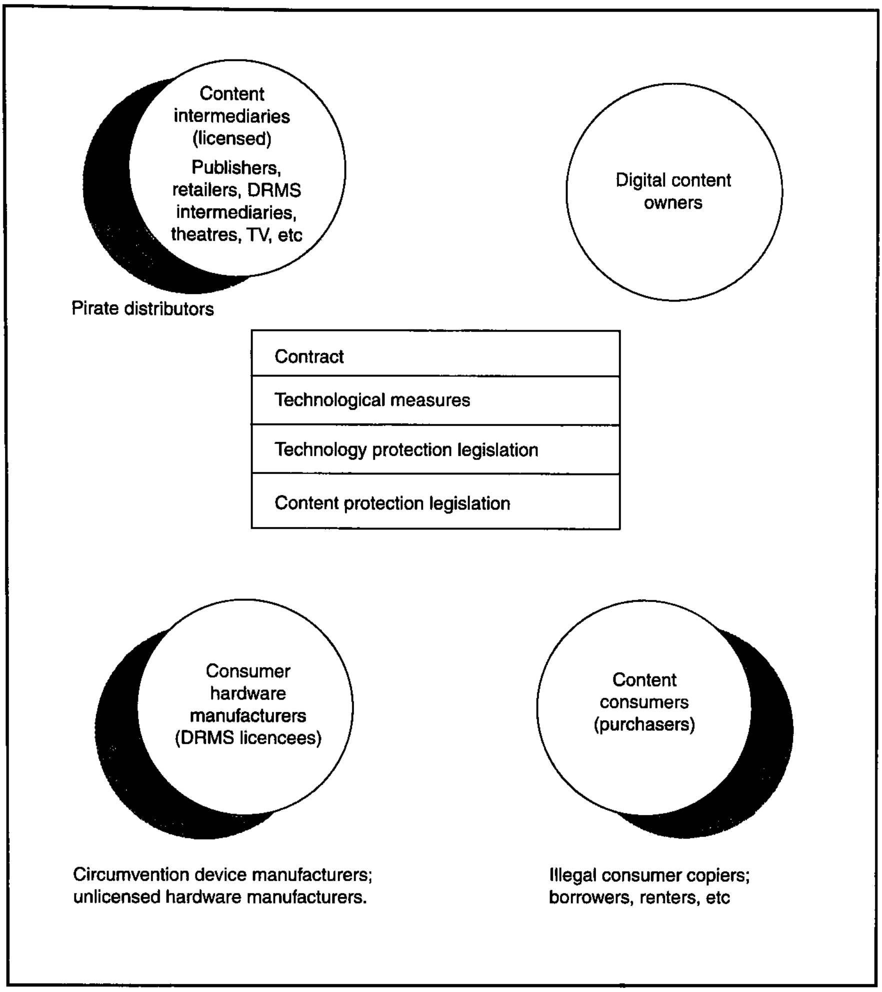
Online surveillance through the use of "cookies"[16A] and "web bugs"[16B] (single pixel gifs) has already become a contentious privacy issue, but these examples relate more to marketing uses of our browsing habits than to the conditions of use of IP.

Our rights to limit surveillance via artefacts will become one of the key privacy issues for the start of this century, with surveillance by digital works likely to be one of the most contentious and common examples.

[16] Apple's iMusic software and its use of the CDDB database is one example.

[16A] "A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time." (from *Whatis?com* definition), *see* http://searchSecurity.techtarget.com/sDefinition/0,,sid14_gci211838,00.html.

[16B] "A Web bug is a file object, usually a graphic image such as a transparent one-pixel-by-one pixel GIF, that is placed on a Web page or in an e-mail message to monitor user behavior, functioning as a kind of spyware. Unlike a cookie, which can be accepted or declined by a browser user, a Web bug arrives as just another GIF on the Web page. A Web bug is typically invisible to the user because it is transparent (matches the color of the page background) and takes up only a tiny amount of space." (from *Whatis?com* definition), *see* http://searchWebManagement.techtarget.com/sDefinition/0,,sid27_gci341290,00.html.


Content intermediaries (licensed)
Publishers, retailers, DRMS intermediaries, theatres, TV, etc
Pirate distributors
Digital content owners
Contract
Technological measures
Technology protection legislation
Content protection legislation
Consumer hardware manufacturers (DRMS licencees)
Circumvention device manufacturers; unlicensed hardware manufacturers.
Content consumers (purchasers)
Illegal consumer copiers; borrowers, renters, etc

The new paradigm for content protection

The new paradigm which is emerging for the protection of digital content is not simply a matter of technology being used to protect copyright works. It is summarised in the diagram below, which can be used to represent the relationships between content owners and the three types of parties whose conduct they need to regulate in order to maintain control over the content they provide, and obtain revenues from it. Four distinct methods of regulating those relationships are now used, in complex combinations.

The three types of parties are:

1 *Content consumers* – Content owners aim to ensure that the end-users of their works observe any requirements that the content owner imposes on the use of the work, including payment conditions. As well as consumers who have purchased copies, content owners want to

enforce these conditions against other users such as illegal copiers and borrowers.

2 *Consumer hardware manufacturers* – Content owners need to ensure that manufacturers of hardware that present their digital works are consistent with and do not circumvent any content protection technologies they use with their works. They want to stop any hardware manufacturers from making or dealing in hardware that will circumvent their content protection measures.
3 *Content intermediaries* – Content owners also need to ensure that those who distribute their content do not distribute pirate copies, or do anything that interferes with their content protection measures.

In order to obtain the protection that content owners want in relation to digital content, they are relying on complex combinations of at least four different forms of protection (possibly six, if different types of contracts are distinguished).[17] These are:

1 *Technological measures* – CPT and DRMS are used to protect digital content and metadata (RMI).
2 *Contract* – Content owners aim to enter contracts wherever possible with each of the other three types of parties:
   a *"Click-wrap" contracts with consumers* – In contrast to the past, the use of DRMS allows content owners to require content consumers to enter a contract before using a digital work, provided courts uphold the validity of "click-wrap licences".[18] Since it is possible to include such click-wrap contracts in any on-line system, digital artefact, or even hardware device, it is theoretically possible for content owners to ensure that all "users" of a work, including those who borrow it to make an unauthorised copy of it, enter into a contract with the copyright owner, making the provisions in a DRMS-protected contract resemble a property right.[19]
   b *DRMS technology licences with hardware manufacturers* – As Bechtold has made clear, these licences are a crucial part of the protection required by content owners before they will agree to distribute their content in a format required by a particular DRMS.[20] This diagram

[17] The following analysis is influenced most strongly by Bechtold (n 13 above), though many other authors have argued similarly. Bechtold adds the emphasis on technology licensing of hardware manufacturers to previous analyses. The author has generalised the approach he takes at a number of points.

[18] A contract entered into by the consumer being required to agree to contractual terms, by clicking an "I agree" button with a mouse, before the consumer can access the digital work; *see ProCD, Inc v Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) for the most significant US decision.

[19] *See* Bechtold (n 13 above), part 3 and part 5.1.2 for a summary of this argument.

[20] *Ibid.*, part 4.

is an over-simplification in this respect, because the DRMS developer is really a distinct party, but assumed here to be acting in accordance with the content providers' wishes (as Bechtold suggests is likely).

c *Distribution licences with intermediaries* – Content owners can use contracts with intermediaries licensed to distribute their content to ensure that technological protections are not weakened and RMI not removed at the distribution stage, including to a stronger extent than is protected by technology protection laws.

3 *Technology protection laws* – Laws prohibiting acts of circumvention of technology protecting digital content or metadata, or making, dealing in or possessing such circumvention devices are not copyright law but a new adjunct to it.

4 *Content protection laws* – Depending on how effective these other protections are, the significance of copyright law may be reduced. Bechtold concludes that "the protection by traditional copyright law plays only a minor role as a safety net".[21] Database protection laws (required in Europe but uncommon elsewhere) may also be relevant, so this element is best called "content protection laws".

These protections are mutually supportive in complex ways. Technology protection laws stop technological measures from being circumvented. The comprehensive coverage of contract relationships with end-users can only be achieved because technological measures stop the avoidance of "click-wrap" contracts.

The same paradigm is being used to protect content which is not protected by copyright law, including the items of content in a database and works which are in the public domain.

Most aspects of the very complex legal issues raised by the combinations of these various protective measures are beyond the scope of this article, which focuses only on the relationship between privacy protection and two of these elements (technological measures and technology protection laws).

CPT

There are a wide variety of particular technologies and products which can be used to protect digital content (CPT). They can be distinguished from *systems* of content protection which are built around one or more of these technologies and involve particular sets of participants (DRMS).

[21] *Ibid.*, part 8.

These CPT can be categorised in various ways. Koelman and Helberger distinguish those that control access, those that control certain uses, those that protect the integrity of a work and those that enable metering of access and / or use.[22]

For the purposes of this article, some of the more important of the variety of CPT[23] can be ranked in approximate order of their implications for privacy (less to more):

1 *Cryptographic "containers"* which allow copies of works to be distributed widely but only used in full once a key has been obtained,[24] or use other metering methods restricting use without further payment ("superdistribution").[25]
2 *Self-limiting works* are works which "refuse" to allow actions which breach the licence conditions of that particular copy of the work (part of Stefik's "trusted systems").[26]
3 *Digital watermarks* (and other forms of steganography) which embed irremovable (and sometimes undetectable) information about rights holders and / or licensees in each copy of the work.
4 *"Trusted printing"*, where a work will not print (or otherwise copy) unless payment is first made for the copy, the work is sent to the "printer" in encrypted form, and the copies are watermarked in some way. These are part of "trusted systems".
5 *Self-destructing works* are works that cease to be useable after the expiration of a licence or a breach of licence conditions, or until a further licence is obtained.
6 *Surveillance through use of existing Internet search engines* to search for infringing copies of works, using normal text searching techniques.

[22] *See* part 2 of Kamiel Koelman and Natali Helberger, *Protection of Technological Measures*, Report under the Imprimatur project (Institute for Information Law, University of Amsterdam, 1998), available at http://www.ivir.nl/publications/koelman/technical.pdf.

[23] This summary draws on discussions from the following articles: Koelman and Helberger (*See* n 22 above); Roger Clarke and Gillian Dempsey, "Electronic Trading in Copyright Objects and Its Implications for Universities", Australian EDUCAUSE'99 Conference, Sydney, 18–21 Apr 1999, http://www.anu.edu.au/people/Roger.Clarke/EC/ETCU.html; Mark Stefik, "Shifting The Possible: How Trusted Systems And Digital Property Rights Challenge Us To Rethink Digital Publishing" (Spring 1997) 12 *Berkeley Technology Law Journal* 1, http://www.law.berkeley.edu/journals/btlj/articles/12_1/Stefik/html/reader.html; Julie Cohen, "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them", (1997)12 *Berkeley Tech. L.J.* 161, http://www.law.berkeley.edu/journals/btlj/articles/12_1/Cohen/html/reader.html; International Federation of Reproduction Rights Organisations (IFRRO), Committee On New Technologies, *Digital Rights Management Technologies*, was, but no longer at http://www.ncri.com/articles/rights_management/.

[24] For example, works protected by Softlock are freely copyable and partially readable "demos", but become full-featured once a password is purchased. They automatically revert to demos when copied to another machine. Softlock's advertisement says: "turn pirates into distributors". Was on http://www.softlock.com/, June 1998, now deleted.

[25] Brad Cox, "Superdistribution" *Wired Archive* 2.09, Sept 1994, http://www.wired.com/wired/archive/2.09/superdis.html.

[26] *See* Stefik (n 23 above) and Mark Stefik, *The Internet Edge* (Boston: MIT Press, 1999).

7 *Customised "web spiders"* that routinely trawl the web for information identifying digital works (eg digital watermarks and other identifiers). Such web spiders are in use[27-29] by Broadcast Music Inc (BMI) and by Digimark, a photo watermarking company acting on behalf of clients such as Playboy.

8 *Self-recording works* are works that record details of when they are used (including breaches of licence conditions). The International Federation of Reproduction Rights Organisations' (IFRRO) ideal system is for "detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on", so that it "captur[es] a record of what the user actually looked at, copied or printed".

9 *ID controls on central access* to works in a central location, which require a *password* or some other form of identification before they can be accessed.

10 *Continuous monitoring of usage by online works* using cookies and web bugs to track all usage of online works resident on a publisher's computer system. Cookie data will identify the user to the publisher each time the user accesses a webpage, and web bugs (or "single pixel gifs") can have a similar effect if a user's IP address can be correlated with an individual user.

11 *Continuous monitoring by works resident on a user's system* of works that, whenever they are online, send reports back to a central location online concerning when they are used or copied, including to obtain "permission" to do so ("IP phone home"). IFRRO's[30] ideal system sends "this usage record ... to the clearinghouse when the user seeks additional access, at the end of a billing period or whenever the user runs out of credit."

This is an unsystematic and incomplete list of illustrations. Although there are a bewildering variety of techniques and products that we could classify as CPT, from the perspective of their significance for privacy protection, most seem to combine a few basic elements:

1 *Access controls* – Controlling access to a work may be as simple as requiring a password or only accepting http requests that come from particular sub-domains, or it may require authentication of the enquirer by a digital signature. Where copies of works are distributed, each copy

[27-29] Charles C. Mann, "Who Will Own Your Next Good Idea?" *The Atlantic Monthly*, Part II, (Sept 1998), http://www.theatlantic.com/issues/98sep/copy2.htm.

[30] International Federation of Reproduction Rights Organisations (IFRRO), *see* http://www.ifrro.org/.

may require a separate encryption key to access it (eg "cryptolopes"). Works may be such that they "refuse" to allow various forms of use (printing, "cut and paste", use beyond a certain date, etc) unless certain conditions are met. These are more sophisticated forms of access control.

2 *Identification in the work* – There are many techniques for embedding meta-information (information about the work) in the work itself, and many types of information embedded, from static information identifying the work, its licensee or licence conditions, to dynamic information that is updated as the work is used.

3 *Surveillance* – Whatever technologies are used, rights owners (or intermediaries representing them) often need some form of active surveillance of access to and use of the work, either in order to utilise their rights under copyright law, or for the digital work to execute its own remedies (eg "refusing" to operate), or to grant or refuse licences. The information needed is typically stored in the work itself, but the rights-owner must access it either through "pull" methods (eg search engines and web spiders) or "push" methods (eg cookies and other means of sending data back to a central point).

DRMS

Individual CPT are important, but they are not the key element in the cyberspace architecture that is being developed to protect IP. What may make architecture replace law as the principal protection of digital works is a common framework for the trading of IPR, both between businesses and to end-users, a set of standards within which all of the particular CPT can work.

DRMS may take many forms, depending in part on which combination of CPTs are employed. In addition, the business models which will become commercially successful are still emerging.

The "ideal aims" of a DRMS have been described (in a formulation more sympathetic to consumer and privacy rights than most product descriptions)[31] as follows:

1 to provide copyright-protected material to users upon request;
2 to provide a means for remuneration (or a facility to grant or refuse a licence) to flow to the owner;
3 to track usage of material (which documents, how often, used by whom and so on) without interfering with the privacy of the user;
4 to prevent unlawful appropriation of the copyright material by people who are outside the system;

[31] Was on Australia's Cultural Network site at http://www.acn.net.au/resources/ip/ecms.htm, now deleted.

5 to prevent unlawful use of the copyright material by users who obtain the material legitimately in the first instance;
6 to ensure the integrity of the IP;
7 to allow for a reasonable flow of information between owners to users (owners are often also users and vice versa) in the public interest (that is, a DRMS should not unreasonably tie up the community's information and cultural resources); and
8 to allow for the effective operation of fair dealing within the DRMS.

The potential for privacy intrusions is apparent from the third, fourth and fifth aims, even in this "ideal" description.

A description of one of the best-known early DRMS models, the European Imprimatur Project,[32] illustrates how some fundamental changes to the way in which copyright currently operates would follow from the implementation of such a DRMS:

1 Each digital work is issued with *a unique identification number*,[33] which is then inserted by the content provided as microcode in the work to enable it to be tracked in various situations. See below concerning the range of identification systems emerging.
2 There is *an intellectual property rights (IPR) database*, "somewhat similar in content and function to a land title registry", enabling anyone (particularly potential purchasers) to verify a digital work's identification and legal status.
3 There is a *monitoring service provider* (MSP) which, on behalf of creators and rights holders, will (though the summary does not say this) monitor transactions, uses and breaches (depending on the technology) of rights in digital artefacts. MSPs will use a variety of mechanisms,

[32] In Europe, the Imprimatur project, sponsored by the European Commission (EC), developed the Imprimatur Business Model. Bygrave and Koelman (n 10 above) describe the actors and inter-relationships in the model at p 3:

> "In brief, the role of the creation provider (CP) is analogous to that of a publisher; ie, he / she / it packages the original work into a marketable product. The role of the media distributor (MD) is that of a retailer; ie, he / she / it vends various kinds of rights with respect to usage of the product. The role of the unique number issuer (UNI) is analogous to the role of the issuer of ISBN codes; ie, it provides the CP with a unique number to insert in the product as microcode so that the product and its rights-holders can be subsequently identified for the purposes of royalty payments. The role of the IPR database provider is to store basic data on the legal status of the products marketed by the MD. These data concern the identity of each product and its current rights-holder. The main purpose of the database is to provide verification of a product's legal status to potential purchasers of a right with respect to usage of the product. As such, the IPR database is somewhat similar in content and function to a land title register. The role of the monitoring service provider (MSP) is to monitor, on behalf of creators / copyright-holders, what purchasers acquire from MDs. Finally, the certification authority (CA) is intended to assure any party to an ECMS operation of the authenticity of the other parties whom he / she / it deals. Thus, the CA fulfils the role of trusted third party (TTP)."

[33] *See* Bygrave and Koelman (n 10 above), p 7.

including reporting from Media Distributors, and surveillance of the web through the use of search engines, customised web spiders, and digital artefacts that report on their own usage.

4 *Certification Authorities* (CAs) play a major role, as it is assumed that both parties to transactions, and the authenticity of communications from them will be routinely identified by digital signatures, and so verification by CAs is needed.

This blueprint for the networked DRMS architecture in which IP transactions will operate in cyberspace could hardly be more different from the current world of books, videos and CDs. As regulation, this "code" (in Lessig's terminology) shares few similarities with IP law. This is not necessarily a criticism, merely an observation of how powerful and different architecture as regulation will be in IP.

Standards and pervasiveness

The success, importance and privacy dangers of networked DRMS is likely to depend, in large part, on the extent to which they achieve interoperability between multiple publishers (within one DRMS), and ultimately, between different DRMS and different media types. The greater the degree of interoperability, the greater the potential for aggregation of personal information concerning our consumption of digital content.

One of the key standards is for identification of digital works. Gervais[34] described 11 competing standards, including a variety of media-specific identifiers, and more general proposals such as the Digital Object Identifier (DOI)[35] and Persistent Uniform Resource Locators (PURLs).[36] He also described five standards for metadata[37] that (in the absence of one global identification system for digital works emerging) might provide a basis for

[34] Daniel J. Gervais, "Electronic Rights Management and Digital Identifier Systems" (1998) 4(2), *The Journal of Electronic Publishing*, http://www.press.umich.edu/jep/04-03/gervais.html (visited 22 June 1999).

[35] "A DOI (digital object identifier) is a permanent identifier given to a Web file or other Internet document so that if its Internet address changes, users will be redirected to its new address. You submit a DOI to a centrally-managed directory and then use the address of that directory plus the DOI instead of a regular Internet address. The DOI system was conceived by the Association of American Publishers in partnership with the Corporation for National Research Initiatives and is now administered by the International DOI Foundation. Essentially, the DOI system is a scheme for Web page redirection by a central manager." (from *Whatis?com* definition), *see* http://whatis.techtarget.com/definition/0,,sid9_gci213897,00.html.

[36] "Functionally, a PURL is a URL. However, instead of pointing directly to the location of an Internet resource, a PURL points to an intermediate resolution service. The PURL resolution service associates the PURL with the actual URL and returns that URL to the client. The client can then complete the URL transaction in the normal fashion. In Web parlance, this is a standard HTTP redirect." (from PURL homepage), *see* http://www.purl.org/.

[37] Dublin Core, US MARC, INDECS Project, Stanford Digital Library Metadata Architecture, BIBLINK/NEDLIB.

interoperability between DRMS based around different numbering systems. DOI and PURL also have the potential to unify differing numbering systems without replacing them.

This Babel of identifications for digital works is as yet slowing down the development of networked DRMS, and this slow development buys a limited amount of time for privacy protection to be developed.

Privacy and Related Issues in CPT and DRMS

Online surveillance of users of digital works involves a variety of privacy dangers which are summarised in this section, starting with the most general, and proceeding to issues of technology design.

Monitoring of reading and viewing habits poses the threat of *a "chilling effect" on freedom to read, think and speak*. Cohen describes it as "a giant leap ... toward monitoring human thought".[38] Bygrave and Koelman argue that "[t]he attendant, long-term implications of this for the vitality of pluralist, democratic society are obvious".[39]

The collection of information on reading and viewing habits creates risks of the misuse of personal information for *secondary purposes*, particularly, but not only, marketing purposes. These risks are amplified if those collecting personal information can aggregate data from our reading / viewing different sources, so as to construct profiles. The use of reading / viewing information for marketing purposes is obvious. Non-marketing examples of unacceptable

[38] Julie Cohen, speaking mainly of the IFRRO's notion of an ideal DRMS, concludes in Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'copyright management' in Cyberspace", (1996) 28 *Conn. L. Rev.* 981, http://cyber.law.harvard.edu/property/alternative/Cohen.html:

> "These capabilities, if realized, threaten individual privacy to an unprecedented degree. Although credit-reporting agencies and credit card providers capture various facets of one's commercial life, CMS raise the possibility that someone might capture a fairly complete picture of one's intellectual life.
>
> Reading, listening, and viewing habits reveal an enormous amount about individual opinions, beliefs, and tastes, and may also reveal an individual's association with particular causes and organizations. Equally important, reading, listening, and viewing contribute to an ongoing process of intellectual evolution. Individuals do not arrive in the world with their beliefs and opinions fully-formed; rather, beliefs and opinions are formed and modified over time, through exposure to information and other external stimuli. Thus, technologies that monitor reading, listening, and viewing habits represent a giant leap – whether forward or backward the reader may decide – toward monitoring human thought. The closest analogue, the library check-out record, is primitive by comparison. And library check-out records are subject to stringent privacy laws in most states." (footnotes omitted).

[39] Bygrave and Koelman (n 10 above), while not opposed to DRMS, stress that the surveillance dangers are one of the most significant obstacles to their acceptable operation:

> " ... such systems could facilitate the monitoring of what people privately read, listen to, or view, in a manner that is both more fine-grained and automated than previously practised. This surveillance potential may not only weaken the privacy of information consumers but also function as a form for thought control, weighing down citizens with "the subtle, imponderable pressures of the orthodox", and thereby inhibiting the expression of non-conformist opinions and preferences. In short, an ECMS could function as a kind of digital Panopticon. The attendant, long-term implications of this for the vitality of pluralist, democratic society are obvious."

secondary uses are that researchers or lawyers do not want anyone to know what digital works they are consulting, and an author wanting permission to include an extract in an anthology or other collection does not want his or her publishing plans indirectly disclosed to rival publishers.

Minimising unnecessary identification is a significant issue. There is a need to maximise the use of CPT which *allow anonymous transactions* involving digital works, provided that in doing so we don't create worse problems of unfair contract enforcement (see below). Otherwise, when it is necessary for transactions to be potentially identifiable, *pseudonymity* needs to be used wherever possible,[40] to prevent the misuse of personal information for secondary purposes, and also to prevent a "chilling effect" on freedom to read, think and speak.

Intermediaries between users and rights owners will play a crucial role in safeguarding and administering pseudonymity, and in aggregating usage information for publishers and authors without interfering with user privacy.[41] Many CPT can be and will be used without any intermediaries between the end-user of a digital work and the rights-holder. "Disintermediation" was one of the buzzwords of Internet business models. In its positive incarnations, we think of recording artists or authors being able to sell directly to *their* publics. Just as likely, publishing houses of various sorts (still the rights-holders) will

[40] Gervais (n 34 above) describes the role of pseudonymity in the proper operation of DRMS:

> "A related issue is how to identify individual digital copies (which presumably have been sold to a specific user), without creating a risk to privacy or confidentiality. If indeed individual copies are identified, using a watermark containing a transaction code for instance, a viable solution could be to number individual copies, without including data identifying the user who 'ordered' the copy in question. Copy numbers could be linked, in a secure database, to the individual users. Should there be a good reason to make the link between the copy number and the user – for instance, under court order – that link could be made. The role of trusted third parties acting as aggregators of usage data might be especially important to users. An aggregator or collective management organization using an electronic copyright-management system could thus maintain the confidentiality of the link (if any) between a given copy delivered on-line and a specific user. The content owner would receive with the payment for use of his works a report on the number of uses, possibly with an indication of the type of users concerned, but no information about individual users. Without this type of confidentiality guarantee, it may be very difficult for electronic copyright commerce to prosper. In other words, properly tuned electronic copyright-management systems that aggregate data so as to protect privacy and confidentiality are probably essential ingredients of the success of electronic copyright commerce."

[41] Gervais (n 34 above), a proponent of DRMS, emphasises the crucial role that DRMS intermediaries (such as MSPs and CAs in the Imprimatur model) will have in the protection of privacy:

> "An electronic copyright-management system does not in and by itself protect privacy, but it is probably the best tool to do so. If the rules under which the electronic copyright-management system operates are correctly designed, the system would return to rights holders aggregated information on use of his / her works. For example, the system could say that clearance was granted to use 'Scientific Article X' to '11 pharmaceutical companies in the last month', or that '2,345 users in this part of Chicago' downloaded a given musical work. The rights holder thus gets market data without violating anyone's confidentiality or privacy. Even now the Copyright Clearance Center in the U.S. does not report to rights holders which articles from medical or scientific journals are used by individual users (eg., pharmaceutical companies). It only tells rights holders how often a work was used by, say, the pharmaceutical industry as a whole. Most collective management organizations aggregate information in this way and this is perhaps a function whose value has thus far been underestimated by users."

do a far greater percentage of direct selling to *the* public without the use of intermediaries such as booksellers. Online booksellers could also develop into intermediaries for digital works in a DRMS model. The result is likely to be a mixture of delivery models, but the point is that a lot of CPT and DRMS will be run directly by publishing houses with lots of different products to shift and a strong interest in secondary use of identified consumption data, or by booksellers with a similar combination of interests. We will not always be "lucky" enough either to have some central industry-based monitoring body standing between consumers and publishers trying to act as an "honest broker", or to be dealing directly with the author who has only his or her own product to sell. Which business models succeed will have a significant effect on privacy.

Related Consumer Issues: "Fair Use" and Fair Enforcement

Privacy is not the only issue raised by DRMS, nor perhaps even the most important one. The architecture of DRMS need not observe any of the public interest limitations built into copyright law. These include the right to lend a work for use by others (the basis of libraries – the "first sale doctrine"), and the various "fair dealing" rights to copy works or parts thereof for purposes such as "criticism and review" or "private study and research". As Lessig puts it, "what the law reserves as a limitation on the property holder's rights the code could ignore".[42] If dealings in relation to digital works become direct transactions where it is practical for the rights-owner to enter into a contract with the user (unlike the purchase of a book in a store), then such contracts are likely to routinely exclude such public interest exceptions. As observed earlier, fair use was traditionally exercised in private, so privacy interests are also relevant here.

The enforcement of such contracts is also unlike real space contracts, Lessig points out,[43] because whereas the law always takes into account various public and private interests in determining the extent and means by which contracts will be enforced, when contracts are self-enforced by code (for example, by the work suddenly becoming unusable) these public values are not likely to be taken into account. We might add that when the law enforces a contract, there is an independent assessment of whether there has been a breach of the contract, whereas here the enforcement is automated and unilateral, built into the architecture. If "code contracts" replace law, these are not necessarily the same as "law contracts", and may not be in the public interest. There is also likely to be an overlap with privacy interests here, because of the surveillance involved in determining where there has been a breach.

[42] Lessig (n 5 above). Lessig also notes an extensive argument in the US as to whether "the fair use exceptions to copyright protection are not affirmative rights against the copyright holder, but instead the consequence of not being able to efficiently meter usage. Once that technical limitation is erased, then so too would the fair use rights be erased."

[43] Lessig (n 5 above).

Laws Against Circumvention – Beyond Copyright?

The recent amendments to copyright legislation in some jurisdictions which provide legislative prohibitions against copyright circumvention devices and against the removal of RMI are implementations of the WCT and the WIPO Performances and Phonograms Treaty (WPPT). National implementations of the Treaty are the first general legislative protections given to CPT and DRMS, by the negative device of preventing their circumvention or removal.[44] There have previously been less systematic or general attempts in some jurisdictions, amounting to a "modest body of law".[45]

Although often phrased in terms of protecting copyright, they are of broader significance as one means by which authors can protect an expanded set of rights beyond copyright through a combination of contracts, technology and surveillance.

The WCT

Article 11 of the WCT[46] provides, in relation to copyright circumvention devices:

> "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restricts acts, in respect of their works, which are not authorised by the authors concerned or permitted by law."

Article 12 of the WCT provides, in relation to RMI:

> "(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:
> (i) to remove or alter any electronic RMI without authority;
> (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic RMI has been removed or altered without authority.

[44] They are also an instance of laws facilitating surveillance which we can describe as "data surveillance law."

[45] Koelman and Helberger (n 22 above), part 3.1 note a number of US, UK and EU provisions which deal only with some types of circumvention, or specific types of works.

[46] The WIPO Performances and Phonograms Treaty, Art 18 is a very similar provision, but the discussion in this paper will only refer to the WCT, Art 11.

> (2) As used in this Article, 'rights management information' means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public."

From the perspective of privacy protection, some of the questions we need to ask are whether these provisions and their national legislative implementations allow persons to:

1. delete from digital works personal information that facilitates surveillance;
2. prevent a web robot from looking for infringing artefacts; or
3. prevent a digital work from communicating information over the Internet.

Hong Kong and Australia as Examples of Implementation

National implementations of the WCT are what is crucial, and they may take a conservative or an expansive approach to what the WCT requires. In the following sections, we will take Australia and Hong Kong as examples of implementation.

In 1998, the Australian government announced its plans to ban commercial dealings in circumvention devices and to ban removal of RMI.[47] The proposed amendments drew heavily on what was then the proposed European Commission (EC) Directive.[48] The amendments to the Copyright Act 1968 (Cth) by the Copyright Amendment (Digital Agenda) Act 2000 have been in force since March 2001.

The Hong Kong SAR has provisions with the same intent in sections 273–274 of the Copyright Ordinance (Cap 528) which was enacted in 1997, shortly after the finalisation of the WCT.

The United States' Digital Millennium Copyright Act (DMCA) of 1998 has amended Title 17 of the US Code (dealing with copyright) to implement the WCT. The EC Directive on Copyright in the Information Society, which

[47] *See* Commonwealth Attorney-General's Discussion Paper *The Digital Agenda* (1998) "Part 5 – Proposed scheme for new technological measures and rights management information provisions", http://law.gov.au/publications/digital.htm#anchor1565870. *See* also Speech by Attorney-General D. Williams, "Copyright and the Internet: New Government reforms", para 35, Murdoch University, 30 Apr 1998, http://law.gov.au/articles/copyright_internet.html.

[48] Proposed EC Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society – *see* Arts 6 and 7 – now Directive 2001/29/EC.

deals with anti-circumvention and RMI issues primarily in Articles 6 and 7, was passed in May 2001.[49] Both are only mentioned briefly by way of comparison, particularly where they take a different approach to privacy-related issues.

Anti-circumvention – Australian and Hong Kong Provisions

Australia

Section 116A provides[50] that a copyright owner or exclusive licensee has a right of action (section 116A(5)) against a person who makes, sells or otherwise deals in various specified ways with "a circumvention device[51] capable of circumventing, or facilitating the circumvention" of "technological protection measures", or a "circumvention service"[52] with a similar capability. Defendants are only liable if they knew or ought reasonably to have known that the device or service would be used "to circumvent, or facilitate the circumvention of, the technological protection measure" (section 116A(1)).

[49] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (O.J. L 167, 22 June 2001, p 10 *et seq.*); for analysis, *see* Bygrave (n 12 above) and Kamiel Koelman, "A hard nut to crack: The protection of technological measures" (2000) *European Intellectual Property Review* 227, draft available at http://www.ivir.nl/publications/koelman/hardnut.html.

[50] Section 116A(1) sets out the scope of the right:
"s116A(1) Subject to subsections (2), (3) and (4), this section applies if:
(a) a wor̦k or other subject-matter is protected by a technological protection measure; and
(b) a person does any of the following acts without the permission of the owner or exclusive licensee of the copyright in the work or other subject-matter:
(i) makes a circumvention device capable of circumventing, or facilitating the circumvention of, the technological protection measure;
(ii) sells, lets for hire, or by way of trade offers or exposes for sale or hire or otherwise promotes, advertises or markets, such a circumvention device;
(iii) distributes such a circumvention device for the purpose of trade, or for any other purpose that will affect prejudicially the owner of the copyright;
(iv) exhibits such a circumvention device in public by way of trade;
(v) imports such a circumvention device into Australia for the purpose of:
...;
(vi) makes such a circumvention device available online to an extent that will affect prejudicially the owner of the copyright;
(vii) provides, or by way of trade promotes, advertises or markets, a circumvention service capable of circumventing, or facilitating the circumvention of, the technological protection measure; and
(c) the person knew, or ought reasonably to have known, that the device or service would be used to circumvent, or facilitate the circumvention of, the technological protection measure."

[51] Section 10 defines "circumvention device": "*circumvention device* means a device having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure."

[52] Section 10 defines "circumvention service": "*circumvention service* means a service, the performance of which has only a limited commercially significant purpose, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an effective technological protection measure."

A "technological protection measure" means (section 10):

> " ... a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject-matter by either or both of the following means:
>
> (a) by ensuring that access to the work or other subject-matter is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright;
> (b) through a copy control mechanism."

Where section 116A applies, the copyright owner may obtain an injunction, damages (including additional damages) or an account of profits (section 116D). There is also a criminal offence where the same conditions as in section 116A are satisfied, but with a higher burden of proof ("reckless" rather than "ought reasonably to have known") and with the onus of proof on the Crown (sections 132(5A)–(5B)). A similar offence is created in relation to the operation of a "circumvention service" (sections 132(5C)–(5D)).

Hong Kong

Hong Kong's anti-circumvention provisions[53] are very different from Australia's in form. Section 273 provides remedies against "a person who, knowing or having reason to believe that it will be used to make infringing copies" deals with (in various ways) or possesses "for the purpose of, in the course of, or in connection with, any trade or business, any device or means specifically designed or adapted to circumvent the form of copy-protection employed" or "publishes information intended to enable or assist persons to circumvent that form of copy-protection". "Copy-protection" includes "any device or means specifically intended to prevent or restrict copying of a work or fixation of a performance or to impair the quality of copies or fixations made".

Anti-circumvention: Analysis of the Provisions

The effects of section 116A (Australia) and of section 273 (Hong Kong) are complex, particularly in relation to privacy interests. In the points following, the author attempts to identify some of the main implications, and unresolved issues, arising from section 116A, and compare them with the equivalent position in section 273.

[53] References following are to the Copyright Ordinance (Cap 528).

Users will usually be liable, even though the act of circumvention is not a breach

In Australia, it is not a breach of section 116A to use a circumvention device, or to possess one. Nor is the act of circumvention itself covered by these provisions. Only making and dealing in such devices is proscribed. Similarly, although provision of a "circumvention service" is actionable (and a criminal offence), it is not actionable (or an offence) simply to use such a service. Similarly, in Hong Kong it is not a breach of section 273 to use a circumvention device *per se*. It is a breach to possess such a device knowing it will be used for circumvention, but only if this is "in the course of, or in connection with, any trade or business" (section 273(2)(a)). "Private", non-business possession is, therefore, outside the Hong Kong provisions, but possession by business users is included. In contrast, both the DCMA and the EC copyright Directive prohibit the act of circumvention (with some exceptions).

However, it is misleading to think that users in Hong Kong and Australia will not usually be liable for acts of circumvention. The use of a circumvention device will involve liability for breach of copyright by the user, if it involves the making of an infringing reproduction ("copies" in Hong Kong terminology). This may occur in two ways.

First, many, if not most, digital works cannot be used without a transient copy of the work being made by the hardware device used to display the work. However, in Australia, in some cases, such as playing movies embodied in DVDs, these transient copies will not constitute a "copy" under section 10: *Australian Video Retailers v Warner*.[54] In addition, section 43A provides that, even where the transient copying of a work (literary, dramatic, musical or artistic) which occurs during use is a reproduction, it is not an infringement if it is made "as part of the technical process of making or receiving a communication" (unless "the making of the communication is an infringement of copyright"). While this means that web browsing does not infringe copyright, it does not assist a user who is using a circumvention device which results in a reproduction (even if temporary) being made of a copyright work. The user would be liable for a copyright infringement unless a defence applied (such as one of the fair use defences), the work was in the public domain, or an implied licence still applied.[55] The Australian situation is, therefore, complex.

In Hong Kong, section 65 provides that transient copies of every type of subject matter are not infringing if "technically required for the viewing or listening of the work by a member of the public to whom a copy of the work is made available", despite section 23 providing that such copies are infringements. This implies that, provided a user has legitimately obtained a

[54] *Australian Video Retailers Association Ltd v Warner Home Video Pty Ltd* [2001] FCA 1719.

[55] It seems unlikely that an implied licence would still operate under circumstances of attempted circumvention.

copy of a work, making a temporary copy of it for purposes of viewing or listening, in the course of use of a circumvention device, would not constitute infringement. Even where section 65 does not apply, there might be no infringement by playing DVDs, despite section 23(6),[56] because no "making of copies" is involved: *Australian Video Retailers v Warner*.

Second, it is quite possible that the use of a circumvention device will require the copying and / or adaptation of software or data comprised in the CPT / DRMS which is protected by copyright. Such copying will probably fall outside the protection for transient copies (section 65 and section 43A discussed above) because it is not for "receiving a communication" or "viewing or listening". It does not come within the exceptions for copying software for such purposes as error correction in either the Hong Kong or Australian legislation.[57] However, some uses of circumvention could arguably involve copying programs in ways which are "for the purposes for which the program was designed" (Australia, section 47B) or "necessary for the lawful use of the program" (Hong Kong, section 61). In both jurisdictions, use of the circumvention device could result in an infringing copy of software, but it is difficult to generalise.

Furthermore, a question remains as to whether a person who writes his or her own small piece of software in order to prevent some surveillance device operating as it is intended might be regarded as "making" a device.

An additional risk is that, where a digital work is provided online by someone else, use of a circumvention device or service to obtain unauthorised access to a computer system could also involve criminal offences.[58]

We can conclude that, although use of circumvention devices is not explicitly prohibited, in both Australia and Hong Kong, users need (but do not have) a positive statutory "right to circumvent" in order to be able to safely access a digital work for purposes which would provide a defence to an action for infringement. Such a right should be provided by law.

"Upstream" prohibitions can make user rights meaningless

The focus on the "upstream" providers of circumvention devices or services in both Australia and Hong Kong, rather than the "downstream" use of such devices or services (or circumvention *per se*) appears at first to be one of the most significant limits on the scope of these provisions, though as we have already seen that users will often be liable.

However, as Koelman argues in the European context, "too broad a prohibition on preparatory activities would render the permission to circumvent

[56] Section 23(6) states: "Copying in relation to any description of work includes the making of copies which are transient or are incidental to some other use of the work".

[57] Sections 60–61 Hong Kong and ss 47AB–47H Australia.

[58] The scope of the "computer crime" laws of Australia and Hong Kong is not covered in this article.

meaningless"[59]. The discussion following supports this hypothesis in relation to Australia and Hong Kong.

Effects much broader than preventing copyright breaches

Under section 116A (Australia), the essence of a breach is to make or deal in a device / service capable of circumventing or facilitating the circumvention of a "technological protection measure", knowing or reasonably suspecting it would be so used. For a number of reasons, this provision can be used to prevent conduct which has little to do with a breach of copyright.

First, in the definition of "technological protection measure", provided that an "access control" or "copy control" measure does have some effect in "inhibiting" copyright infringements, it is not necessary that this should be its primary purpose. Many access control or copy control mechanisms would at least "inhibit" copyright infringement unless it was nearly or totally ineffective. "Inhibit" must include something less than "stop", otherwise "prevent" would have no meaning in the section. However, if a CPT is only aimed at preventing something which is not a breach of copyright (such as playing DVDs: *Australian Video Retailers v Warner*) then it will not constitute a "technological protection measure".[60] So the scope of "technological protection measure" is very broad but with very large holes.

Similarly, it does not matter that a "copy control mechanism" also stops the copying of content that is not protected by copyright (eg public domain material, or individual items in a database) or stops copying in circumstances which would not be a breach of copyright because defences apply.

The use of"‘"designed" in that definition implies that a device must be intended by its designer to protect copyright, and not merely inadvertently do so (as any computer security device might do). It must have some effectiveness.[61]

Second, knowledge or belief that infringement of copyright will take place is not required by section 116A, only knowledge or belief that a technological protection measure will be circumvented. If it were believed that the circumvention device was only going to be used in relation to public domain works, or data items in a database, this would not be an excuse.

Third, although only a copyright owner or exclusive licensee can take action (section 116A(5)), it is sufficient if they have one copyright work protected by the relevant device being circumvented, even if no one intends

[59] Koelman (n 49 above). "Preparatory activities" means the making of and dealing with circumvention devices, the "upstream" activities.

[60] I am indebted to John McPhail on this point: personal communication on file with author.

[61] If a device is intended to protect copyright works, but is in fact quite ineffective to do so, is it still a "technological protection measure"? This does not matter because, following the WTO Treaty, there is only a "circumvention device if it has the purpose of circumventing an *effective* technological protection measure" (s 10 definition of "circumvention device").

to use the device to circumvent protection in that work. Copyright owners can, therefore, commence actions which are really intended to protect technologically protected content which does not have copyright protection.

In Hong Kong, the defendant is only liable if he or she deals with or possesses the circumvention device "knowing or having reason to believe that it will be used to make infringing copies or infringing fixations". If a particular defendant (for example a library) possesses a device only for the purpose of allowing "fair dealings" of works (sections 38 and 39), then this is not a breach. If a defendant has a reasonable belief that a device in which he or she is dealing (or possesses) will only be used for circumventions in relation to works in the public domain (including those in which copyright has expired), or database items in which there is no copyright, or any content in relation to which a defence applies, then there will be no breach in the making or dealing. In addition, uses of circumvention devices which do not involve any copies being made, but (for example), merely prevent the collection of personal information for privacy-protection purposes, will not be a breach.

The Hong Kong provisions are a more careful and cautious implementation of the WCT requirements, and are tied much more closely to the protection of copyright-protected content and actions than are the Australian provisions.

Defences effectively removed in Australia

In Australia, as explained above, it is not a defence to an act of circumvention that involves an incidental infringement of copyright, nor to the supply of a circumvention device, that the user's purpose would otherwise give a defence to an infringement action (such as the "fair dealing" defences in sections 40–43). Circumvention, not infringement, are what is important.

There are various provisions allowing supply of circumvention devices for some purposes to libraries, archives, educational institutions, the Crown, law enforcement agencies, etc.[62] These exemptions involve the approved type of institution making a declaration to the provider of the circumvention device identifying the category of exemption and stating that "a work ... to which the person proposes to use the device ... is not readily available to the person in a form that is not protected by a technological protection measure".

However, these exemptions do not include the "fair dealing" defences (sections 40–43), of use for research or study, criticism and review, reporting news, or providing professional advice. Fair uses, and the privacy of fair use, are not recognised by this legislation.[63] In order to preserve the effective exercise of "fair dealing" rights, the "right to circumvent" suggested above is needed.

[62] *See* s 116A(3)–(4A) and (7)–(9). There is a separate national security exemption in s 116A(2).

[63] Compare Cohen (n 38 above), Part V "The First Amendment Case Against the Proposed Anti-Tampering Law".

As discussed above, in Hong Kong, dealing in a circumvention device without reason to believe it would be used for infringing uses would not be a breach, and nor would possessing it in the course of a business. Use of a device for a non-infringing purpose is not a breach, because use does not cause liability. The Hong Kong legislation is, therefore, better than the Australian legislation on this point. However, in practice, the lack of availability of circumvention devices may mean that most users of digital works who would be theoretically entitled to take advantage of fair use exemptions will be unable to do so.[64]

Liability for publishing information about circumvention

Hong Kong imposes liability if a person "publishes information intended to enable or assist persons to circumvent that form of copy-protection" (section 273(2)(b)). The use of "intended" will raise difficult questions concerning some publications (eg academic papers and technical reports) which could have such an effect.

Another problem would be a website which provides links to overseas websites where circumvention devices may be downloaded. In the United States, eight motion picture companies have brought a case against *2600 Magazine* to enjoin it from publishing or linking to DeCSS, a computer program used to circumvent the encryption used in DVDs, and other similar cases have been commenced, but none concluded.[65] The case is being defended on the grounds that the anti-trafficking provisions of the DMCA are unconstitutional because they infringe First Amendment freedom of speech rights. Like the United States, consideration needs to be given to whether section 273(2)(b) is inconsistent with the protection of freedom of expression in the Hong Kong Bill of Rights Ordinance (Cap 383), on the basis that it goes beyond what is "necessary" to protect the rights of others.[66] It would also be necessary to take into account Article 34 of the Basic Law providing that "Hong Kong residents shall have freedom to engage in academic research, literary and artistic creation, and other cultural activities". At the least, these provisions should lead to a narrow reading of section 273(2)(b).

In Australia, there are prohibitions on anyone who "by way of trade ... otherwise promotes, advertises or markets, such a circumvention device" (section 116A(1)(ii)) or "makes such a circumvention device available online to an extent that will affect prejudicially the owner of the copyright" (section 116A(1)(vi)), or provides or promotes a circumvention service, if "the per-

[64] Compare Koelman (n 49 above), "Preparatory activities".

[65] For a review and current status of all of the "DeCSS cases", *see* the "OpenLaw: Open DVD" forum at http://eon.law.harvard.edu/openlaw/DVD/ (Berkman Centre, Harvard Law School).

[66] Art16(3), s 8 Hong Kong Bill of Rights, Bill of Rights Ordinance (Cap 383).

son knew, or ought reasonably to have known, that the device or service would be used" for circumvention. A person who merely provides information about circumvention devices on a non-commercial basis (eg an academic or technical paper) is unlikely to fall within these provisions. Whether a hypertext link to a circumvention device "makes [it] ... available online" under section 116A(1)(vi) is similar to the more general question of whether providing hypertext links to any work constitutes an infringement of the new right of "making available to the public" under both the Australian and Hong Kong legislation. This is a broader question than can be pursued here, but there is some opinion that links may constitute "making available".[67] Unlike the United States or Hong Kong, there are in Australia no entrenched rights of freedom of speech (outside political matters) which could be used to attack these provisions.

Broad and ill-defined scope of devices covered

In Australia, the definition of "technological protection measure" has been broadened from that in the Bill, so that it now includes "a copy control mechanism" as well as forms of "access control". The access control protection will protect the use of CPT aimed at access limitation such as "crypto-bottling" of works (where access depends on use of a particular decryption key) or the simple device of providing on-line (or CD-ROM) access only by password. Technologies to make digital artefacts expire after use or after a period could also be protected here.

"Copy control mechanism" is undefined, and its possible meaning is most uncertain. It would, for example, include any technology which limits printing from webpages or databases in any way. However, would it include *ex post facto* technological means of detecting copyright infringements, such as the use of web spiders to search for unauthorised copies of digital works? These are not access controls, but could well be considered "a copy control mechanism". The inclusion of surveillance devices as protected technology could have significant privacy implications. Similarly, a digital watermark or similar device of steganography, does not prevent access, but it may well be regarded as "a copy control mechanism" in that it both inhibits copying and allows its detection. Such devices would include a code that a word processor or a hypertext markup language (HTML) editor could put into documents to identify if it was created by a licensed copy of software. The question courts

[67] Ross McLean and Anne Flahvin, "The Digital Agenda Act: how the new copyright law (and contract) is redefining the relationship between users and owners of copyright" (2001) *CyberLRes* 211, http://www.austlii.edu.au/au/other/CyberLRes/2001/21/. *See also* Ross McLean and Anne Flahvin, "Aspects of the New Right to Communicate", UNSW Continuing Legal Education Conference, Nov 2000.

will have to resolve is whether "copy control" includes deterrence or detection. The reference to "inhibit" in the Australian definition supports such an interpretation.

If web spiders are copy control mechanisms, it then becomes a question of whether a website operator can circumvent them without "making" a circumvention device, or obtaining one from someone else who will then be dealing in a circumvention device. At what point will writing a few lines of software to configure a web server differently become "making" a circumvention device?

In Hong Kong, works are protected if they are made available "in any form which is copy-protected" (section 273(1)(b)). Copy-protection "include(s) any device or means specifically intended to prevent or restrict copying of a work or fixation of a performance or to impair the quality of copies or fixations made" (section 273(4)). This will not cover access control mechanisms, except where circumvention of access control does involve the making of copies of a work. The Hong Kong definition only refers to "prevent or restrict", and it is possible that "restrict" might be interpreted as broadly as "inhibit". Alternatively, "prevent" could be interpreted as only meaning "stop copying occurring under some circumstances" in which case it is narrower than "inhibit". If so it seems unlikely that this would include web spiders or steganography, which merely deter copying by increasing the likelihood of detection.

As an example of a possible copy control mechanism, works may be issued on DVDs including a region control coding, and selling DVD players allowing the playing of DVDs from all regions circumvents that control. In situations like this, where works are merely viewed, the question arises as to whether the viewing involves the generation of something sufficiently permanent to constitute a "copy" (for example, the caching[68] of a webpage). Although section 23(6) says that "copying" includes making copies which are transient or incidental to other uses of the work, section 65 provides that "[n]otwithstanding s23, copyright in a work is not infringed by the making of a transient or incidental copy which is technically required for the viewing or listening of the work by a member of the public to whom a copy of the work is made available".

[68] "The files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser (for example, Internet Explorer). When you return to a page you've recently looked at, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic." (from *Whatis?com* definition of "cache"), *see* http://searchWebManagement.techtarget.com/sDefinition/0,,sid27_gci211728,00.html.

Unclear exemption for other commercial purposes

In Australia, circumvention devices and services are restricted to those that have "only a limited commercially significant purpose or use ... other than the circumvention". The section would be clearer if it said "no commercially significant purpose or use". If, for example, a new version of a web browser included useful printing features which incidentally made some forms of inhibiting printing of webpages ineffective, this would seem unlikely to be a circumvention device because the printing feature is otherwise commercially significant. Similarly, if an Internet service provider (ISP) excluded all web robots from its site[69] (which may host many other content sites), and thereby excluded some which were searching for copyright-infringing content, then this would not be a breach (even if – as discussed above – such a robot were a "technological protection measure") because such a service or exclusion has many other commercially significant purposes and uses, such as reducing system load. However, if an ISP "made" and used software which excluded only those robots which searched for IP infringements, it might be a different matter.

The Hong Kong prohibition on dealing with devices is limited to "any device or means specifically designed or adapted to circumvent the form of copy-protection employed" (s273(2)(a)). This limitation to devices "specifically designed" to circumvent will serve to exempt devices which have more general purposes but incidentally defeat a form of copy protection.

Surveillance of users' computers may be authorised

A digital artefact resident on a user's PC can be designed so that it cannot be accessed or copied unless there is first an online check back to the copyright owner's database to confirm that the licence allows this and is still valid (The author calls this "IP, phone home"). This could be regarded in Australia as either an "access ... process" or "a copy control mechanism" protected by section 116A. Making or providing devices or services to prevent this surveillance will be illegal even if the personal information which is collected by the technological device is used primarily for secondary purposes (eg marketing) which have nothing to do with copyright protection. This will be so even if the main reason the information is collected is for marketing purposes, because the surveillance will still have some effect in "inhibiting" copyright infringements. Furthermore, the circumvention will be illegal whether or not normal privacy protections in the collection of personal information have been observed.

[69] The Robot Exclusion Protocol is observed voluntarily by most commercial web spiders, *see A Standard for Robot Exclusion*, http://www.robotstxt.org/wc/norobots.html, and "A Method for Web Robots Control" (an "Internet Draft", a working documents of the Internet Engineering Task Force, 1996, expired June 1997), http://www.robotstxt.org/wc/norobots-rfc.html. Site administrators have the technical capacity to exclude specific robots from their site compulsorily if they do not obey the protocol.

One of the most far-reaching forms of surveillance by and of digital works is, therefore, protected against circumvention – it will be illegal to assist users to circumvent such surveillance. The EC Copyright Directive provisions on anti-circumvention raise similar problems of interpretation.[70]

Such collection may be in breach of privacy laws, though this is not certain (see the next section). As a matter of policy, anti-circumvention provisions should not provide protection for any technological measures that do not meet privacy protection standards required by legislation. The DMCA provides an explicit defence against its anti-circumvention provisions where circumvention is only for the purpose of protection of personally identifying information, but the protection can be defeated by "conspicuous notice".[71]

Other variants of online surveillance of users might be less clearly within the definition of "technological protection measures". For example, a digital artefact that recorded its own usage even when offline, and then (once it went online) sent this information "home" so that users could be charged for usage, or for detection of breaches of licence conditions (such as copying or printing), probably would not be regarded as an access control mechanism, but could still be argued to be a copy control mechanism, if "control" is interpreted to include deterrence or detection.

Under the Hong Kong provisions, it is less clear whether digital artefacts on a user's PC that send information "home" when they are online are protected against circumvention. As discussed above, it seems that many devices attempting to prevent unauthorised access to any online or CD-ROM access to works will be covered, because of the wide definition of "copy-protection". However, as with Australia, protection of the recording of usage details and *ex post facto* reporting of them when the artefact goes online will depend on whether "copy-protection" is interpreted to include deterrence and detection, but this is less likely in Hong Kong. Also, in Hong Kong, a circumvention device must be used to make infringing copies, and devices that block surveillance are unlikely to do this.

If (despite the above argument) online surveillance of usage is regarded as a copy protection device in Hong Kong, any protection for users against secondary usage of the information (such as marketing uses) will depend on Hong

[70] Bygrave (n 12 above) says the Directive "provides no obvious answer".

[71] *See* US Code Title 17Sec 1201 (i) *Protection of Personally Identifying Information*, providing that it is not a breach to circumvent "the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person" if the following conditions are satisfied:
"(a) the access controls collect or disseminate information about the online activities of a person;
(b) conspicuous notice about this information processing is not given;
(c) the data subject is not provided the ability to prevent the information being gathered and disseminated; and
(d) the disabling of the controls has the sole effect, and is solely for the purpose, of preventing the collection and dissemination."

Kong's privacy laws, as the Copyright Ordinance does not itself impose any limits on use of the information collected.

Conclusions

In summary, in most respects the Hong Kong anti-circumvention provisions are narrower than the Australian provisions, as they tie the protection of technology more closely to breaches of copyright. This approach is preferable to the Australian provisions which can far more easily result in the anti-circumvention provisions being breached in circumstances having little to do with breaches of copyright.

Protection of Rights Management Information (RMI) – Australia and Hong Kong

Australia

In relation to RMI, section 116B of the Copyright Act 1968 provides a right of action to the copyright owner or exclusive licensee where "a person removes or alters any electronic rights management information attached to a copy" of copyright subject matter without permission and where "the person knew, or ought reasonably to have known, that the removal or alteration would induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter" (which knowledge is presumed by section 116B(3)).

Additional actions in relation to commercial dealings with copyright subject matter from which RMI has been removed are provided in section 116C, where the relevant knowledge is that the person knew, or ought reasonably to have known, that the removal of the RMI "would induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter" (which knowledge is presumed by section 116C(3)).

Criminal offences equivalent to the actions in section 116B and section 116C are provided in section 132(5D) which makes it a criminal offence to "remove or alter any electronic rights management information attached to a copy of a work", provided there is the required intent,[72] and in section 132 (5D) which provides related offences concerning distributing, importing and communicating artefacts where such information has been removed or altered.

[72] Section 132(5D) provides:

> "(5C) A person must not remove or alter any electronic rights management information attached to a copy of a work or other subject-matter in which copyright subsists, except with the permission of the owner or exclusive licensee of the copyright, if the person knows, or is reckless as to whether, the removal or alteration will induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter."

"Electronic rights management information" is defined in section 10 in terms very similar[73] to those in Article 12(2) of the WCT and Article 19 of the WPPT:[74]

> *Electronic rights management information* means:
> (a) information attached to a copy of a work or other subject-matter that:
> (i) identifies the work or subject-matter, and its author or copyright owner; and
> (ii) identifies or indicates some or all of the terms and conditions on which the work or subject-matter may be used, or indicates that the use of the work or subject-matter is subject to terms or conditions; and
> (b) any numbers or codes that represent such information in electronic form.

Hong Kong

The Hong Kong Copyright Ordinance, section 274, includes a definition of RMI which is essentially the same as the WCT and Australian definitions in its effect, though different in its wording. "A person who provides rights management information" has the same rights and remedies as a copyright owner has in respect of an infringement of copyright against a person who "removes or alters any electronic rights management information provided by him without his authority". The definition of RMI is in effect the same as in Australia.[75]

RMI: Analysis

The Hong Kong and Australian provisions are similar in relation to their effect on user privacy in most respects.

Identifying information can be RMI

The Australian section 10 definition of RMI does not explicitly refer to information identifying the user (the owner of the copy of the work in most cases).

[73] Though the Australian provision conjoins (a)(i) and (a)(ii) with "and", not "or".

[74] WIPO Performances and Phonograms Treaty.

[75] Section 274(3). References in this section to RMI mean:
"(a) information which identifies the work, the author of the work, the owner of any right in the work, the performer, or the performance of the performer;
(b) information about the terms and conditions of use of the work, the person having fixation rights in relation to the performance, or the performance; or
(c) any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or a fixed performance or appears in connection with the making available of a work or a fixed performance to the public."

Bygrave and Koelman question whether the WTC definition includes information identifying users such as the Purchaser ID (in the Imprimatur model).[76] The WCT, Australian and Hong Kong definitions of RMI all include "conditions" on which a work may be used. If a work has been licensed on the basis of a "single user" licence to a specified individual, it is hard to see why the identity of that individual is not part of the conditions of use. If this is correct, then any information about users that is a necessary part of a condition of use is RMI and cannot be removed (provided it is "attached") without breach of the RMI provisions.[77] However, any information about users that is not a necessary part of a condition of use is not RMI and can be removed. In comparison, the DMCA provisions defining "copyright management information" imply that any information concerning users is not included.[78]

Information transmitted is not RMI

The definition of RMI in both Australia and Hong Kong only includes information which is "attached" to the work. The protection of RMI would, therefore, not extend to the prevention of blocking the online transmission of RMI back to some central collection point ("IP , phone home") each time the work is used. This interpretation is also supported by the use of "remove". The RMI provisions, therefore, protect the passive storage of RMI, but not its active dissemination. The WTC, Article 12, requires protection of information which "appears in connection with the communication of a work to the public" as well as to "attached information", but this does not seem to require protection of information sent back to a central collection point.

RMI does not include information about actual usage

The definition of RMI in both the WTC, Article 12, and section 10 (Australia) does not refer to information about actual usage of a work, but only to its "conditions" of use. Ongoing collection of actual usage information by a digital work is, therefore, not RMI and can be removed. The two references in the Hong Kong provisions to the RMI being "provided" by the copyright owner make it even more clear that RMI protection does not extend to any data about the actual usage of works (as distinct from usage conditions), because such data would be "provided by" the user (even if unknowingly), not by the copyright owner.

[76] *See* Bygrave and Koelman (n 10 above), p 53.

[77] Compare Bygrave and Koelman (n 10 above), p 53.

[78] *See* US Code Sec 1202 *Integrity of copyright management information*, providing that "copyright management information" includes "terms and conditions for use of the work" and "such other information as the Registrar of Copyrights may prescribe by regulation, except that the Registrar of Copyrights may not require the provision of any information concerning the user of a copyright work".

"Self-help" for privacy protection is not allowed

The Australian provision prohibits removal of RMI "except with the permission of the owner of the copyright", and Hong Kong prohibits removal without the authority of the person who provided the RMI. Article 12 of the WCT only requires prevention of removal "without authority", and Bygrave and Koelman[79] argue that in the European Union (EU) context such authority could come from what is permitted or required by law (such as laws implementing the EU Privacy Directive).

This might not seem to matter if (as argued above) RMI does not include personal information (except perhaps the identity of a licensee where this is a necessary part of the conditions of use of a work), so removal of such information is not a breach of the RMI provisions.

Nevertheless, removal of such "pseudo-RMI" might require the use of an (unobtainable) circumvention device, or if the user attempts to modify the work to prevent the collection of this "pseudo-RMI", this may be a breach of copyright, so the pseudo-RMI may be protected. The user still needs some positive right similar to that found in the United States' DCMA, at least in Australia. In Hong Kong, devices to remove RMI are less likely to be circumvention devices because circumvention devices must make infringing copies (as discussed above).

Conclusions

The Australian and Hong Kong RMI provisions seem to avoid the worst threat to privacy in that they do not make it compulsory for users to accept active surveillance and reporting by digital artefacts that reside on their computers, because they exclude most such personal information from the definition of RMI. Nevertheless, they leave users defenceless against the *de facto* implementation of such surveillance, giving them no positive right to remove such pseudo-RMI if to do so involves copyright breaches, and no right to obtain the necessary circumvention devices to do so.

Conclusions – the Cumulative Effect of Anti-circumvention and RMI on Privacy

We can summarise some of the above discussion with some tentative answers to the questions with which we started:

1 *May you delete personal information that facilitates surveillance from digital works?* In both Australia and Hong Kong, if the information is necessary as part of the terms of a user licence, you probably cannot because it is protected RMI. Other personal information is not protected as RMI. In both jurisdictions, the removal of other personal information

[79] *See* Bygrave and Koelman (n 10 above), p 53; *see also* Koelman (n 49 above).

would not *per se* be actionable under the anti-circumvention provisions. In Australia, anyone dealing in devices to assist its removal could possibly be liable for dealing in circumvention devices, but in Hong Kong this is less likely because circumvention is more closely tied to infringement of copyright.

2 *May you prevent a web robot from looking for infringing artefacts?* General methods of excluding robots are exempted from being circumvention devices under both jurisdictions as they have other significant commercial uses. If only "IP bots" are excluded, then in Australia it is uncertain whether a code to achieve this could constitute a circumvention device or service to circumvent "copy control". In Hong Kong it is unlikely.

3 *May you prevent a digital work from communicating information over the Internet?* Under Australian and Hong Kong law, it is possible that some forms of such communication will be an "access ... process" protected against circumvention, and if not they could be "copy protection". Other communications by digital works that merely report on usage but do not control access may be protected against circumvention if copy protection is taken to include deterrence or detection (again, less likely in Hong Kong). Personal information in the process of communication does not constitute RMI because it is not "attached" to the work at that point.

These examples indicate that laws facilitating technological protections of copyright could have a very substantial impact on privacy interests, and that significant issues need to be resolved, particularly in Australia, but less so in Hong Kong. There is a need for a positive right to remove "pseudo-RMI" in both jurisdictions. Even in Australia, the implementation of the WTC provisions does not go so far as to constitute an unrestricted "licence for surveillance" of our hard disks and usage habits. But it seems that the essential surveillance task, online checking of entitlement to use digital artefacts, is protected against circumvention. IP can phone home to check that it should still be at your place, and there are very considerable limits to what you or others can do to stop it.

The Effects of Privacy Laws on Technical Protection of IP

Having considered the extent to which copyright laws are facilitating surveillance, we now need to complete the picture by asking to what extent do existing data protection and privacy laws impose limits on the operation of CPT and DRMS in order to protect privacy?

Hong Kong and Australia are two of the few jurisdictions outside Europe with data protection (or "personal information protection") laws which cover the private sector.[80] Hong Kong's Personal Data (Privacy) Ordinance (Cap 486) has been in force since 1995, and Australia's Privacy Act 1988 (Cth) has applied to significant parts of the private sector since December 2001.

Since the implementation of the EC copyright Directive in May 2001, European countries must implement both anti-circumvention / RMI laws and data protection laws.[81] Bygrave and Koelman have each made a number of studies of the interrelationship between European privacy laws and anti-circumvention / RMI laws.[82]

The experience of the United States is of limited relevance here. The United States is unlikely to enact comprehensive data protection laws, partly for constitutional reasons.[83] The DMCA has explicit provisions limiting the operation of the anti-circumvention and RMI-protection provisions where they would infringe privacy, as mentioned above. Arguments that laws prohibiting copyright circumvention devices diminish "the right to read anonymously"[84] and may breach the guarantees of freedom of speech and privacy in the US Constitution are of limited relevance as legal arguments in countries such as Australia which do not have such constitutional guarantees. These arguments, which are still unresolved in the United States, have some potential relevance in Hong Kong, due to the limited protection of freedom of speech in the Hong Kong Bill of Rights Ordinance and the entrenchment of the International Covenant on Civil and Political Rights by the Basic Law. Most European and some other countries are more willing than the United States[85] to protect privacy by general information privacy legislation, and do not have the same constitutional constraints in doing so.[86]

Is DRMS Data "Personal Information"?

Most data protection laws only protect "personal data" or "personal information", requiring that the information be capable of being linked to an

[80] New Zealand and Canada are the other significant examples.

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23 Nov 1995, p 31 *et seq.*).

[82] *See* Bygrave and Koelman (n 10 above), particularly Ch 2; Koelman (n 49 above); and Bygrave (n 12 above).

[83] Michael Froomkin, "The Death of Privacy?" (May 2000) *Stan. L. Rev.* 146, draft available at http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

[84] Cohen (n 38 above).

[85] In many other countries, there is likely to be less reluctance to interfere in "private orderings" of transactional relationships concerning IP by legislation, for example by compulsory licensing schemes. Even in the United States, compulsory terms in such contractual relationships are not so unusual. William W. Fisher stresses that compulsory terms in contracts are not at all unusual in the US, and proposes a set of such compulsory contractual terms for contracts concerning IP rights: *see* William W. III Fisher, "Property and contracts on the internet" (1998) 73 *Chicago – Kent Law Review* 1203, draft at http://www.law.harvard.edu/Academic_Affairs/coursepages/tfisher/compuls99.htm.

[86] Froomkin (n 83 above).

identifiable individual. However, legislation usually allows the data in question to be combined with other data to produce this identification, but expresses how this combination may be achieved in different ways. For example, in Australia's Privacy Act 1988 (Cth) "personal information" means any information "about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" in question (section 6). Hong Kong's definition is similar.[87]

In many cyberspace transactions, what will constitute "personal information" is uncertain, and this may have a severe effect on the applicability of data protection laws to those transactions. In Australian law, whether machine addresses and e-mail addresses would constitute personal information would usually be a question of fact in a particular case.[88] Bygrave and Koelman also thought this was uncertain.[89]

In the DRMS context, there may be many doubtful situations. For example, if a web spider merely collects the identification number of a licensed digital work, but it is possible for that identification number to be subsequently correlated (perhaps via a number of steps) with the identity of the individual who holds the licence, has the web spider been involved in the collection of personal information? Questions may also arise whether, if part of the information is accessible to the public on a webpage, the combined information can still be "personal information", but this will depend on the wording of particular legislative provisions.[90]

However, these types of definitions may miss the real point of many cyberspace interactions. If a DRMS can determine that a copy of a digital work it has located on the net (or which has reported to it) is an infringing copy, or is being used in breach of its licence, and it can initiate enforcement action without knowing the identity of the person who is responsible, it has acted against an individual and with serious consequences. For example, if a digital work merely sends "back to base" information about the PC on which it is located, or the Internet sub-domain on which it resides, but there is no record in the rights-owner's database of a licence in relation to those locations, so that the work automatically ceases to be useable, where is the collection or use of personal information? Similarly, if information about the reading habits of a pseudonymous licensee can be aggregated so that it is commercially

[87] Section 2 defines "personal data":

> " 'personal data' means any data-
> (a) relating directly or indirectly to a living individual;
> (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
> (c) in a form in which access to or processing of the data is practicable".

[88] Graham Greenleaf, "Privacy principles – irrelevant to cyberspace?" (1996) 3 *PLPR* 114, http://www.austlii.edu.au//au/other/plpr/vol3No06/v03n06d.html.

[89] *See* Bygrave and Koelman (n 10 above), p 14.

[90] *See* Greenleaf (n 2 above), Part F "Stopping Searching – Robot Exclusion Standards" for discussion.

valuable to market other digital works to that individual, and there is access to an e-mail address which makes this possible, the publisher has no need to know the identity of the individual marketed to.

This weakness in definitions of personal information may place a significant limit on the capacity of data protection laws to protect privacy in relation to surveillance systems used for copyright protection.

Anonymity and Pseudonymity as Privacy Rights

It is possible for many aspects of DRMS and CPT to be designed so that pseudonymity (and in some cases anonymity) of licensees can be preserved, while still protecting the core economic interests of rights-holders. However, the secondary economic interests of rights-holders (or intermediaries) in being able to exploit the personal information that they obtain from DRMS are in direct conflict with rights of anonymity and pseudonymity. Issues of purpose specification will be crucial. DRMS intermediaries can use pseudonymity in order to maintain their ability to identify copyright infringements of digital artefacts, while preventing secondary use of the identifiable information by rights owners. Many authors have identified the availability of pseudonymous transactions as a key element of the design of DRMS that protect privacy.[91]

In Australia's privacy law, National Privacy Principle (NPP) 8 "Anonymity" requires that "[w]herever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation". This "anonymity principle" is unusual in data protection laws,[92] but does have a precedent in Germany.[93] It is not explicitly required by the EC data protection Directive.[94] Although the title of NPP 8 only refers to anonymity and not pseudonymity, the words "not identifying themselves" are broad enough to encompass systems which allow pseudonymity, with actual identification only being permitted under certain conditions.

[91] *See* for example Graham Greenleaf, "'IP, phone home' ECMS, (c)-tech, and protecting privacy against surveillance by digital works" Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 1999, Proceedings text available online at http://www.pco.org.hk/english/infocentre/files/greenleaf-paper.doc, HTML version available at http://austlii.edu.au/~graham/publications/ip_privacy/; Jonathan Weinberg, "Hardware-Based ID, Rights Management, and Trusted Systems" (2000) 52 *Stan. L. Rev.* 125, http://www.law.wayne.edu/weinberg/newstanford.PDF.

[92] Its Australian origins lie in Principle 10 of the Australian Privacy Charter (1994): "People should have the option of not identifying themselves when entering transactions" (*see* Australian Privacy Charter Council (1994) Australian Privacy Charter, http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html). In 1998, the Australian Privacy Commissioner's *National Principles for the Fair Handling of Personal Information* included Principle 8 as now appears in the Act (with "should" in place of "must").

[93] *See* n 96 below and accompanying text.

[94] There is debate within the EC as to whether it is implied by the Directive (personal communication with Lee Bygrave); *see* Bygrave (n 12 above) for discussion.

There is no explicit equivalent in the Hong Kong Privacy Ordinance. It would be difficult to read a requirement of pseudonymity or anonymity into the scattered words of Data Protection Principle (DPP) 1,[95] requiring that data collected is "necessary for", "directly related to" or "adequate but not excessive in relation to" the purpose of collection. Similarly, it is unlikely that the words "unless the information is necessary for one or more of its functions or activities" in Australia's NPP 1 would be interpreted to require pseudonymity or anonymity.

One of the few other examples is Germany's Teleservices Data Protection Act (Article 2 of the Information and Communications Services Act of 1997), which requires the objective of minimising or eliminating the collection and use of personal information to be built into the "design and selection of technical devices" (hardware and software):

> "s3(4) The design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible."

This design requirement makes meaningful the specific requirement on service providers to provide anonymous and pseudonymous uses of teleservices "to the extent technically feasible and reasonable",[96] because it removes the excuse that systems have not been designed to allow for anonymous or pseudonymous transactions. Here, the control of architecture by law is both a serious, though general, limitation on the types of Internet systems that may be built, and a necessary precondition for legal sanctions aimed directly at the behaviour of service providers.

One of the main differences between this Australian formulation and that in the German law is that it does not have the explicit legislative requirement for systems to be designed to allow anonymity and pseudonymity. The Australian provision might, therefore, be interpreted to allow the excuse that it is not "practicable" because the system design makes it technically impossible. However, the strong wording of "must have the option" may be interpreted to at least require any systems designed after the legislation commences to provide anonymity and pseudonymity options wherever "practicable".

Data protection commissioners are increasingly aware of the importance of this issue. The Article 29 Working Party of European Data Protection Commissioners made recommendations in 1997 concerning anonymity on

[95] Schedule 1.

[96] "s4(1) The provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable. The user shall be informed about these options."

the Internet[97] which show a clear preference for maximising anonymity in Internet transactions, subject to balancing this with other rights. In 2000, the International Working Group on Data Protection in Telecommunications, drawn from data protection agencies worldwide, specifically recommended the development of DRMS "which allow for anonymous or pseudonymous transactions".[98]

Limits on Collection

The aspect of Australia's NPPs and Hong Kong's DPPs which will have the most direct impact on the operation of copy-protection technologies are the principles governing collection of personal information, NPP 1 (Australia) and DPP 1 (Hong Kong). Various aspects of the collection principles could be relevant.

Collection must be by "fair means and not in an unreasonably intrusive way" (NPP 1.2) or "fair in the circumstances of the case" (DPP 1(2)(b)). Surreptitious use of cookies, web bugs or web spiders could potentially infringe these provisions. Personal data can only be collected if it is "necessary for one or more of [the collector's] functions or activities" (NPP 1) or "necessary for", "directly related to" or "adequate but not excessive in relation to" the purpose of collection (DPP 1).

[97] Art 29 Committee 1997, The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data, *Recommendation 3/97 Anonymity on the Internet* (3 Dec 1997), http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6en.htm.
They recommend that, where appropriate, the "minimum necessary collection" principle "should specify that individual users be given the right of anonymity". A surprising limitation of the working party's approach is that it does not adequately distinguish anonymity and pseudonymity, nor pursue the extent to which pseudonymity should be offered where anonymity is not practicable. The following main conclusions are relevant here:

- The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line.
- Anonymity is not appropriate in all circumstances. Determining the circumstances in which the "anonymity option" is appropriate and those in which it is not requires the careful balancing of fundamental rights, not only to privacy but also to freedom of expression, with other important public policy objectives such as the prevention of crime.

...

- Wherever possible the balance that has been struck in relation to earlier technologies should be preserved with regard to services provided over the Internet.
- The ... purchase of most goods and services over the Internet should all be possible anonymously.

...

- Anonymous means to access the Internet (eg public Internet kiosks, pre-paid access cards) and anonymous means of payment are two essential elements for true on-line anonymity.

[98] International Working Group on Data Protection in Telecommunications 2000, *Common Position on Privacy and Copyright Management* adopted at the 27th Meeting of the Working Group on 4–5 May 2000 in Rethymnon / Crete, http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_en.htm. For the importance of the distinction between anonymity and pseudonymity, *see* Roger Clarke, "Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice", *IFIP User Identification & Privacy Protection Conference*, Stockholm June 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html and Anita Smith and Roger Clarke, "Identification, Authentication and Anonymity in a Legal Context", *IFIP User Identification & Privacy Protection Conference*, Stockholm, June 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/AnonLegal.html.

An important protection of privacy in DRMS systems will be if individuals must be given notice when information is collected about them. In Australia, notice of collection, use and disclosure practices must be given to the individual "at or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual" (NPP 1.3), and "reasonable steps" must be taken to give such notice to the individual even where the information is collected from third parties ("from someone else": NPP 1.5). Hong Kong's DPP 1 has similar provisions, but notice is only required in relation to collection directly from the data subject. In both Australia and Hong Kong, it is questionable whether, when information is collected about a person from a website, or even from the individual's computer, it is collected from "the individual" (Australia) or from "the data subject" (Hong Kong). If it is not so collected, but instead classified as collected from observation / surveillance, no notice is required. The correct interpretation is unresolved, but the better view is that observation of a person, or extraction of information from that person's private computer files (as distinct from pages on a publicly accessible website) should be regarded as collection from the person.[99]

Many aspects of data collection by DRMS will be with the consent of the data subject, or pursuant to a contract with the data subject. They will, therefore, have to comply with the normal requirements of disclosure of purpose, and limitations on excessive collection (as discussed above).[100]

More contentious forms of collection of personal information are likely to arise because of the surveillance aspects of DRMS. If an MSP uses a web spider solely for the purpose of collecting RMI, or if the digital work sends reports back to the MSP, it may be collecting "personal information" (see discussion above). The MSP may be in a contractual relationship with the person concerned (a licensee), but questions may arise as to whether the collection is with consent, or (in EU Directive terms) the collection is necessary for the performance of the contract or for the purpose of the legitimate interests of the MSP or its client. Disclosure of surveillance practices at the time of contract will probably be necessary, as it may be impossible at the time of collection (for example, collection by web spiders).

If the person whose personal information is collected has no relevant contractual relationships (for example, a person whose machine address is disclosed as the location of a digital work), then there will be no consent to collection and no contract, so justification for collection may be more difficult to provide.

[99] *See* Graham Greenleaf, "Key concepts undermining the NPPs – A second opinion" (2001) 8 *Privacy Law & Policy Reporter* 1 for related discussion.

[100] For discussion, *see* Bygrave and Koelman (n 10 above), p 16, also p 27.

Recommendations of the European data protection commissioners

The Working Party on The Protection of Individuals With Regard to the Processing of Personal Data set up under the EU privacy Directive (the Article 29 Committee) made recommendations[101] concerning automated processing which is unknown to the user.[102] All five recommendations are relevant to the collection of data by DRMS and CPT:

1 *Processing of personal data by [digital works] which occurs without the knowledge of the data subject is not legitimate processing (Recommendation 1).* Examples of where this may occur are given above.

2 *Digital works should provide Internet users with information about "the data that they intend to collect, store or transmit and the purpose for which they are necessary"* (Recommendation 2). Where cookies are used, they say, users should be informed in generally understandable language whenever a cookie is to be received, stored or sent. Germany's Teleservices Data Protection Act already provides such a requirement of notification before processing commences (section 3(5)).

3 *Default configurations should not "allow for collecting, storing or sending of client persistent information"*. This means that, in default, browsers should only send the minimum information needed for communication, and should in default refuse to receive cookies (Recommendation 3). Who controls the default settings of cyberspace architecture is one of the key regulatory issues in cyberspace.[103]

4 *Users should be able to "freely decide" about the processing of their personal data, and modify what items are processed* (Recommendation 4).

5 *Users should be able "to remove client persistent information in a simple way"* (Recommendation 5). One problem with applying this to digital works is that it could result in a breach of copyright laws protecting RMI (see discussion above).

Recommendations 3–5 seem inconsistent with many possible implementations of technological protection of digital works, where it is an essential part of the protection of the work that the user does not have a choice but to submit to surveillance as a condition of licensing the work.

[101] Feb 1999. They have not yet been implemented. The recommendations are expressed as applying to "internet hardware and software products". It would be better if they also applied expressly to digital works, as the issues are the same, but it is straining language to call a digital artwork "software". "Digital works" have been substituted for "software" in this discussion.

[102] Art 29 Committee 1999, The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data, *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware* (23 Feb 1999), http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17en.htm/.

[103] *See* Greenleaf (n 2 above).

Limits on Use and Disclosure

The finality principle could have significant implications for the operation of DRMS. NPP 2 in the Australian Act prevents personal information collected by CPT from being used or disclosed for any secondary purpose unless the secondary use is a directly related use which would be reasonably expected, is one given consent, or is one for marketing purposes, and the individual is given the opportunity to "opt-out" from further marketing communications from that organisation. Hong Kong's DPP 2 and section 34 (direct marketing) have a similar effect.

Secondary uses, particularly marketing uses, are analysed by Bygrave and Koelman,[104] who note a number of European provisions which could have a significant effect on DRMS operations.

In relation to automated processing, Article 15(1) of the EU privacy Directive gives persons the right not to be subject to decisions based on automated processing which evaluates information about the personality of the data subject for the purpose of decisions which may have a significant effect on the person.[105] If a CPT terminated the useability of a digital work because of automated processing of information about breaches or expiry of a licence, it could be caught if the information processed included personal information. The processing would have to be shown to be done pursuant to a contract, and even then would have to be within the data subject's reasonable expectations. There is no equivalent protection against automated processing in the Australian or Hong Kong legislation.

Germany's Teleservices Data Protection Act prevents the aggregation in an identifiable form of personal information relating to the use of several teleservices by one user (section 4). Such a restriction would significantly limit the secondary uses of DRMS information. There is no direct equivalent in the Australian or Hong Kong legislation, but it could be questioned whether such aggregation is in itself a legitimate purpose of collection.

Data Export Prohibitions, Extra-Territorial Operation, and Conflicts

DRMS and CPT are likely to involve large-scale flows of personal information between jurisdictions, as many will operate on an international scale with data being collected from users in one jurisdiction by copyright-protection organisations located in another country.

Issues arising from this include the effect of data export prohibition requirements, the possible extra-territorial operation of data protection laws, and questions of conflict of laws. Only the first is discussed here.

[104] Bygrave and Koelman (n 10 above), p 23.

[105] *See* Lee Bygrave, "Minding the machine: art 15 of the EC Data Protection Directive and automated profiling" (2000) 7 *Privacy Law and Policy Reporter* 67.

Data export prohibitions

Where the end-users are located in jurisdictions the laws of which include prohibitions on the export of personal data to countries without adequate privacy laws ("data export prohibitions"), it will be necessary to determine whether any organisation transfers the data to a prohibited jurisdiction, and whether any exemption allowing this applies. Depending on the type of CPT used, there may be information about a particular use of a digital work, or the identity of the user, transmitted via Internet to a collector in another jurisdiction.

As is well known, the EU Data Protection Directive[106] requires European privacy laws to include data export prohibitions. In many instances, the exceptions in Article 26 of the EU Privacy Directive will apply,[107] but there are likely exceptions such as collection by web spiders and other situations where CPT may operate outside contractual relationships.

NPP 9 in the Australian Act prohibits personal data exports to recipients in foreign countries unless one or more exceptions apply. Exceptions are made where the transferor "reasonably believes" the recipient is "subject to a law, binding scheme or contract" which effectively upholds principles substantially similar to the NPPs, where "the individual consents to the transfer", where the transfer is pursuant to certain contract or pre-contractual negotiation, where the transfer is for the individual's presumed benefit (and it is impractical to obtain consent), and where the exporter has taken "reasonable steps" to ensure that the information will not be "held, used or disclosed" contrary to the NPPs.

The data export prohibition in the Hong Kong Ordinance (section 33) is the only section not yet in operation.[108] Its provisions are similar to the Australian NPP 9, but stricter in many respects. The Hong Kong provision only recognises foreign laws, not schemes or contracts. This is particularly important given that the United States (the likely home of many DRMS) does not have privacy legislation but relies upon a voluntary "Safe Harbor" scheme.[109] It only exempts consent "in writing", therefore excluding arguments that consent might be implied by conduct. It does not exempt various types of contracts and negotiations (except insofar as they involve written consent). It requires the exporter to take not only "reasonable precautions", but also to exercise due diligence to ensure that the data will not be "collected, held, processed or

[106] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23 Nov 1995, p 31 *et seq.*).

[107] *See* Bygrave and Koelman (n 10 above), pp 29–31 for detailed analysis.

[108] Hong Kong appears to be waiting until it is clearer how the EU and its member States will interpret and enforce the data export provisions in the Directive.

[109] US Department of Commerce, "Welcome to the Safe Harbor" website http://www.export.gov/safeharbor/.

used" (not only "held, used or disclosed" as in Australia) in ways that would be contrary to the Ordinance. The Australian provision is a "watered down" version of the Hong Kong provision, but it is in force.

In those situations where personal information is transferred to another jurisdiction via the Internet as part of a DRMS, data export provisions could be breached (only in Australia as yet). However, as discussed above (under "Is DRMS data 'personal information'?"), there may be situations where the transfer of DRMS data does not constitute "personal information" or "personal data" and, therefore, falls outside the scope of data protection laws, even though the transfer effectively facilitates the DRMS to react to the situation on an individual basis.

Restoring the Balance – Do We Need Protection from Copyright?

What Privacy Protections Are Needed?

Large-scale implementations of full DRMS are still at an early stage, though many specific CPT are in use. Technologies and business models are yet to mature. It is also too early to be certain how serious the potential risks will turn out to be, as Bygrave warns:[110]

> "Several factors could serve to hinder the large-scale implementation of privacy-invasive DRMS. Such systems might be marginalised by market mechanisms – for example, strong consumer preferences for privacy, combined with competition between copyright-holders to satisfy these preferences. The take-up of privacy-invasive DRMS might also be hindered by difficulties in achieving standardisation and compatibility of technological measures."

It is, therefore, difficult to determine what privacy protections are needed. At the same time, legislation is now giving pro-active protection to CPT and DRMS, through anti-circumvention and RMI laws, so it is too late to do nothing. We need to make the best effort we can to ensure that a balance is maintained (or more likely, restored) between the protection of property and the protection of privacy.

To restore this balance, some of the changes that need to be considered in Australia and (to a lesser extent) in Hong Kong are as follows:

1 Anti-circumvention protections should be tied as closely as possible to the scope of the exclusive rights of a copyright owner, and should not protect subject matter which is in the public domain, is subject to fair

[110] Bygrave (n 12 above).

dealing defences, or merely constitutes access without breach of an exclusive right. Hong Kong's legislation goes close to achieving this. Australia's does not, and should be amended.

2 It should be a defence available to anyone making or dealing in anti-circumvention devices that they have taken reasonable steps to ensure that such devices are used only to circumvent CPT in ways which do not breach an exclusive right of a copyright owner, or do so where a defence against infringement is available.

3 Definitions of "personal information" and "personal data" should be strengthened to apply to more cyberspace transactions affecting individuals, possibly including any transactions allowing interaction with an individual on a personalised basis.

4 Users should be given positive legal authority to remove personal information which has been collected by CPT but goes beyond the requirements of RMI laws ("pseudo RMI"), or is in breach of privacy laws. Blocking or removal of such information should be an exception to copyright laws and to anti-circumvention laws.

5 Users should be given positive legal authority to circumvent wherever they have a defence to an infringement of copyright.

6 Protections of RMI should not require individuals to consent to active on-line surveillance and reporting by digital works on their computers, and privacy laws should prohibit such surveillance.

7 System designers should be required by privacy laws, in the design of DRMS, to allow anonymous transactions where commercial objectives can be met without identification, and allow pseudonymity where it is necessary for transactions to be identifiable in order for commercial goals to be met.

If our laws are to explicitly protect technologies used by copyright owners, then our laws should also give individuals positive rights to protect themselves against those technologies when they breach privacy laws or fail to respect other rights such as rights of fair use.

What Can Privacy Officials Do?

Data protection and privacy commissioners also need to take steps to help maintain or restore the balance between protections of privacy and protections of copyright:

1 They can encourage developers and vendors of CPT and DRMS in their own jurisdiction to develop and publish privacy policies.

2 They should enforce, where appropriate, data protection laws against the local implementations of CPT and DRMS, particularly in relation

to the provision of anonymity / pseudonymity options and excessive collection of information.

3 They should take an active role in local debates on legislation concerning circumvention devices and RMI.

4 They should engage in dialogue and education of the local IP community to ensure that authors, publishers and the public are sensitive to the privacy issues involved in CPT and DRMS. Consumer organisations should be included in any dialogues.