'IP, phone home'
The uneasy relationship between copyright and privacy, illustrated in the laws of Hong Kong and Australia

Graham Greenleaf

Faculty of Law
University of Hong Kong

Law Working Paper Series
Paper No 30

(2001)

'IP, phone home'

The uneasy relationship between copyright and privacy, illustrated in the laws of Hong Kong and Australia

Graham Greenleaf
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
graham@austlii.edu.au

Abstract

Hong Kong and Australia are two of the first jurisdictions in the Asia-Pacific with laws implementing the anti-circumvention and rights management information (RMI) protection provisions arising from the *WIPO Copyright Treaty 1996*.. They are also two of the few jurisdictions outside Europe with privacy (data protection) laws applying to the privacy sector. Their laws illustrate the tensions now arising between copyright and the protection of privacy: property vs privacy.

The development of copyright-protective technologies ('CPT') and electronic copyright management systems ('ECMS'), 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. This paper explores these potential dangers, and possible remedies. How should CPT and ECMS protect privacy interests? How do existing data protection and privacy laws affect the operation of CPT and ECMS? Do laws against copyright circumvention devices and interference with rights management information (RMI) prevent privacy protection?

Version
This is the second version (26 September 2001) of a work-in-progress. The first version (26 June 1999) was presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong 13-15 September 1999, and may be found at http://www2.austlii.edu.au/~graham/publications/ip_privacy/ . Parts 1-3 of this paper are based substantially on the 1999 version.

1. PROPERTY VS 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 libertarians expected intellectual property 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, and technology would win against law and set information free. 'Everything [you know] about intellectual property is wrong' claimed John Perry Barlow[3].

---

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 later concerning the full quote.

2 See Part II of Greenleaf 1998

3 Barlow 1993

The reverse process is now underway: technical protections of intellectual property over networks may protect property interests in digital works[4] more comprehensively than has ever been possible in real space, and destroy many public interest elements in intellectual property 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.

As Lessig observes, infinite copies could only be made if "the code permits such copying", and why shouldn't the code be changed to make such copying impossible'[5]? By 'code' Lessig means software and other aspects of the technical architecture of cyberspace. It has only taken a few years for intellectual property to become one of the most controversial areas where cyberspace architecture is said to be replacing law as the most effective method of protection, due to the emergence of copyright-protective technologies (hereinafter 'CPT') and electronic copyright management systems (hereinafter 'ECMS').

This paper explores what protections are found in information privacy laws against surveillance by digital works, and the extent to which privacy laws need to be strengthened to help provide a reasonable balance between privacy and the protection of intellectual property.

These tensions between property and privacy are illustrated by the laws of Hong Kong and Australia, because they are two of the first jurisdictions in the Asia-Pacific to implement the anti-circumvention and rights management information (RMI) protection provisions arising from the *WIPO Copyright Treaty 1996*. They are also two of the few jurisdictions outside Europe with privacy (data protection) laws applying to the privacy sector. Their laws illustrate the tensions now arising between copyright and the protection of privacy: property vs privacy.

Some specific questions are addressed:

- What are the privacy dangers in CPT and ECMS?
- How should CPT and ECMS protect privacy interests? Do they?
- Do laws against copyright circumvention devices and interference with rights management information (RMI) prevent privacy protection?
- How do existing data protection and privacy laws affect the operation of CPT and ECMS?

This paper asks whether we have only received a fragment of Brand's aphorism[6]: is it really 'Information wants to be free ... but it wants to keep *you* under surveillance' ?

2. ANONYMITY AND PRIVACY - TRADITIONAL IP RIGHTS

We should start with a reminder of some of the ways in which intellectual property laws and enforcement practices have traditionally respected privacy, so as to appreciate better what changes

---

[4] 'Digital works' is used loosely in this article to refer to any digital artefact that could be the subject of copyright, including both 'works' (literary, dramatic, artistic and musical) and other subject matter (films, sound recordings etc).

[5] 'Code Replacing Law: Intellectual Property' in Lessig 1998

[6] One list of famous quotes adds 'Among others. No telling who really said this first.' - <http://world.std.com/~tob/quotes.htm> (visited 15/10/98). 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 - at <http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm>). I'll stick to my imaginary version.

are inherent in new laws and practices. Here are some common, though not universal, features of how users[7] of copyright artefacts experienced copyright law:

- 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.
- 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 why copyright was needed as a property right, since contract was inadequate protection.
- The artefacts had no inherent surveillance capacities. They would not record (much less, communicate) who had used them, when or where.
- Copyright law did not give copyright owners a general right to control uses of artefacts embodying their works, other than the specified '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.
- 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.
- 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.
- 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.
- 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[8]. 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[9]. In comparison, the default condition of anonymity in the normal use of copyright artefacts is more important.

A careful balance was formed over centuries 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[10].

3. TECHNOLOGIES AND SYSTEMS FOR COPYRIGHT PROTECTION

3.1. The networked world of digital artefacts

---

7 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.

8 See Bygrave and Koelman [5.2] for examples.

9 Bygrave and Koelman 1998 emphasise this a little too much in Chapter 5, as does Bygrave 2001

10 As Bygrave 2001 notes, 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'.

Kevin Kelly in 'New Rules for the New Economy'[11] thinks '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."

Surveillance of what we do via the artefacts that we own or use is a much broader privacy issue than copyright protection through technology. Some of the earliest examples have little to do with intellectual property, but often have to do with protection of physical property or of other forms of revenue streams[12].

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. It is also a common tactic of the computer industry is to secretly build artefacts with surveillance capacities enabled in default (at best with some 'opt out' feature) and hope they get away with it.

To see that digital artefacts do live in a networked world is simple enough. Many people now work in offices (or homes) with Internet connections active whenever they are using their computers. This means that every program, document or other file on their computer is (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 an ECMS. Furthermore, many digital artefacts have their full utility only when we 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 PC is online, but not otherwise. The telecommunications infrastructure for digital artefacts to exercise surveillance is

---

[11] Kelly 1997

[12] Here are some examples that are rather more privacy-sensitive than Kelly's, but are not primarily about protecting intellectual property:

- Intel planned to put a machine-specific ID in every Pentium III processor chip, to allow merchants and other "trusted" parties to establish a person's identity (correlated with their machine ID) over networks, and ostensibly to prevent stolen PCs from getting on the Internet (see Lemos 1999). From the intended uses, it is fairly clear how broad the 'unintended' ones could have turned out to be. Intel intended to supply chips with the ID number feature turned on in default, but with a software patch theoretically available for those knowledgeable and persistent enough to wish to protect their privacy - the usual 'opt out' sop. Intel said they would not be keeping a database matching users to their ID numbers - worthless assurances, as they could not control manufacturers of PCs with their chips, or large organisations distributing PCs to users. After a storm of user protest and threatened legislation, Intel said it would turn off the feature by default for remaining unsold chips, converting it to 'opt in'.
- An Australian ISP stopped accepting any dial-ins except from lines that had caller-ID enabled. The ISP claimed it could therefore avoid billing disputes, but the effect on privacy is to make surveillance of dialling location a condition of ISP use.
- Microsoft was forced to change its Windows 98 Registration Wizard after it was shown to be sending a specific hardware identifier to Microsoft without user consent (For Microsoft's admissions, see <http://www.microsoft.com/presspass/features/1999/03-08custletter2.htm>). The following week, Microsoft's Office 97 was shown to include a secret unique identifier (derived from the user's network card) in all documents created with a particular copy. Microsoft claimed that this could not 'reliably' identify the author of a document - a rather unconvincing evasion.

therefore present, and many of us are increasingly making that infrastructure active whenever we are at a computer.

Online surveillance through the use of cookies and 'web bugs' (single pixel gifs) have already become contentious privacy issues, but these are tied more to our browsing habits not to conditions of use of intellectual property.

Our rights to limit surveillance via artefacts will become one of the key privacy issues for the start of this century, and digital works are likely to be one of the most contentious examples. The process of using technologies to protect works is only now starting.

3.2. Copyright-protecting technologies (CPT)

There are a wide variety of particular technologies and products which can be used to protect digital works (hereinafter 'CPT'). We need to distinguish them from *systems* of copyright protection which are built around one or more of these technologies and involve particular sets of participants (an 'electronic copyright management system' or ECMS).

The variety of CPT[13] is summarised[14] below in approximate order of their implications for privacy (less to more):

- Works in a central location, which require a *password* or some other form of identification before they can be accessed.
- *Cryptographic 'containers'* which allow copies of works to be distributed widely but only used in full once a key has been obtained[15], or use other metering methods restricting use without further payment ('superdistribution'[16]).
- *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.
- *Self-limiting works*; works which 'refuse' to allow actions which breach the licence conditions of that particular copy of the work (Stefik's 'trusted systems').
- *'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'.
- *Self-destructing works*, works that cease to be suable after the expiration of a licence or breach of licence conditions, or until a further licence is obtained.
- *Surveillance through use of existing internet search engines* to search for infringing copies of works, using normal text searching techniques.
- *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[17] by Broadcast Music Inc (BMI) and by Digimark, a photo watermarking company acting on behalf of clients such as Playboy.

---

13 For extensive technical papers on various technologies, see Coalition for Networked Information (1994)

14 This summary draws on discussions in from the following articles: Clarke and Dempsey 1999; Stefik 1997; Cohen 1997a; IFRRO

15 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.' - see <http://www.awa.com/softlock/slhome.html>

16 See Cox 1994

17 Mann 1998

- *Self-recording works*; Works that record details of when they are used (including breaches of licence conditions). IFRRO's 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".

- *Continuous monitoring of usage by online works*; 'Cookies' and 'web bugs' can both be used to track all usage of online works resident on a publisher's computer system. Cookie data will identify the user to all the publisher each time the user accesses a web page, 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.

- *Continuous monitoring by works resident on a user's system* Works that, whenever they are online, send reports back to a central location online concerning when are used or copied, including to obtain 'permission' to do so ("IP phone home"). IFRRO's 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. but although there are a bewildering variety of techniques and products that we could classify as CPT, most seem to combine a few basic elements:

- *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 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.

- *Identification in the work* - There are many techniques for embedding meta-information 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.

- *Surveillance* - Whatever technologies are used, rights owners (or intermediaries representing them) often need to 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).

3.3. Electronic Copyright Management Systems (ECMS)

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

An Electronic Copyright Management Systems (ECMS), also known as Digital Rights Management Systems (DRMS), may take many forms. The business models which will become commercially successful are still emerging.

The 'ideal aims' of an ECMS have been described (in a formulation more sympathetic to consumer and privacy rights than most product descriptions)[18] as follows:

- provide copyright-protected material to users upon request;
- provide a means for remuneration (or a facility to grant or refuse a licence) to flow to the owner;

---

[18] Australia's Cultural Network site - at <http://www.acn.net.au/resources/ip/ecms.htm>

- track usage of material (which documents, how often, used by whom and so on) without interfering with the privacy of the user;
- prevent unlawful appropriation of the copyright material by people who are outside the system;
- prevent unlawful use of the copyright material by users who obtain the material legitimately in the first instance;
- ensure the integrity of the intellectual property;
- 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, an ECMS should not unreasonably tie up the community's information and cultural resources); and
- allow for the effective operation of fair dealing within the ECMS.

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

From descriptions of one of the best-known early models, the European Imprimatur Project[19], some fundamental changes to the way in which copyright currently operates can be noted:

- Each digital work is issued with *a unique identification number*[20], 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.

- There is *an IPR database*, 'somewhat similar in content and function to a land title registry', enabling anyone (particularly potential purchasers) to verify a digital work's ID and legal status.

- 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, 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.

---

[19] In Europe the Imprimatur project (<http://www.imprimatur.alcs.co.uk/> visited 15/9/98), sponsored by the European Commission, developed the Imprimatur Business Model. Bygrave and Koelman describe the actors and inter-relationships in the model (Bygrave and Koelman 1998, p3):

> 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).

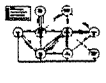

Figure - Imprimatur Business Model (Version 2.0)[19]

[20] Bygrave and Koelman at p7.

- *Certification Authorities* (CAs) play a major role, as it 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 ECMS architecture in which intellectual property transactions will operate in cyberspace could hardly be more different than the real space architecture in which IP operates at present. 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 intellectual property.

Standards and pervasiveness
The success, importance and danger of ECMS is likely to depend in large part on the extent to which they achieve interoperability between multiple publishers (within one ECMS), and ultimately, between different ECMS and different media types.

One of the key standards is for identification of digital works. Gervais[21] described eleven competing standards, including a variety of media-specific identifiers, and more general proposals such as the Digital Object Identifier (DOI) and Persistent Uniform Resource Locators (PURLs). He also describes five standards for metadata[22] that (in the absence of one global identification system for digital works emerging) might provide a basis for interoperability between ECMS based around different numbering systems. DOI and PURL also have potential for unifying differing numbering systems without replacing them.

This Babel of IDs for digital works is as yet slowing down the development of ECMS, and buys a limited amount of time for privacy protection to be developed.

4. PRIVACY AND CONSUMER ISSUES IN CPT AND ECMS

The amount of online surveillance of users of digital works may become unacceptable, compared with the ways in which we use intellectual property in real space.

Some of the main privacy issues are as follows, starting with the most general, and proceeding to issues of technology design:

- Monitoring of reading and viewing habits poses the danger of *a 'chilling effect' on freedom to read, think and speak.* Cohen describes it as 'a giant leap ... toward monitoring human

---

[21] Gervais 1998

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

thought'[23]. Bygrave and Koelman argue that 'The attendant, long-term implications of this for the vitality of pluralist, democratic society are obvious'[24].

- 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 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 her publishing plans indirectly disclosed to rival publishers.

- 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).

- *Pseudonymity* needs to be used wherever possible[25] (when it is necessary for transactions to be potentially identifiable), to prevent the misuse of personal information for secondary purposes, and also to prevent a 'chilling effect' on freedom to read, think and speak.

---

[23] Julie Cohen, speaking mainly of the IFRRO's notion of an ideal ECMS, concludes (Cohen, 1996):

> 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)

[24] Bygrave and Koelman, 1998, while not opposed to ECMS, 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.

[25] Gervais 1998 describes the role of pseudonymity in the proper operation of ECMS:

> 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

- *Intermediaries* between users and rights owners will play a crucial role in safeguarding and administering pseudonymity, and in aggregating usage information for publishers/authors without interfering with user privacy[26]. 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 do a far greater percentage of direct selling to *the* public without the use of intermediaries such as booksellers. Online booksellers like Amazon could also develop into intermediaries for digital works in an ECMS model. The result is likely to be a mixture of delivery models, but the point is that a lot of CPT and ECMS 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 direct with the author who has only her own product to sell.

4.1. Other consumer issues: 'fair use' and fair enforcement

Privacy is not the only issue raised by ECMS, nor perhaps even the most important one. The architecture of ECMS need not observe any of the public interest limitations built in to 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 an limitation on the property holder's rights the code could ignore"[27]. 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.

> 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.

[26] Gervais, 1998, a proponent of ECMS, emphasises the crucial role that ECMS 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.

[27] L Lessig 1998, at 'Code Replacing Law: Intellectual Property'. Lessig also notes extensive argument in the USA 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 to would the fair use rights be erased".

The enforcement of such contracts is also unlike real space contracts, Lessig points out[28], 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.

29303132

5. LAWS AGAINST CIRCUMVENTION OF COPYRIGHT PROTECTION - BEYOND COPYRIGHT

The recent amendments to copyright legislation in many jurisdictions which provide legislative prohibitions against copyright circumvention devices and against the removal of 'rights management information' (RMI) are implementations of the *WIPO Copyright Treaty* 1996 (WCT) National implementations of the Treaty are the first legislative protections given to CPT and ECMS, by the negative device of preventing their circumvention.

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

5.1. The *WIPO Copyright Treaty* 1996

The *WIPO Copyright Treaty* 1996 (WCT) requires contracting parties to Article 11 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 'rights management information':

> (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 rights management information without authority;

---

28 L Lessig 1998, at 'Code Replacing Law: Contracts'.

29 Australia's Cultural Network 'Electronic copyright management systems: what are they? ' - at http://www.acn.net.au/resources/ip/ecms.htm (visited 16/6/1999)

30 <http://www.folio.com/securepub/>

31 <http://www.copyright.com/ >

32 Propagate is at <http://www.propagate.net/>. The model used by Propagate (see <http://www.propagate.net/models.html>), when fully developed, 'has the potential to become a standard in its own right and to be directly implemented in software'. Propagate's objectives are stated to be: 'Propagate is a project to develop through industry, government and community based consensus a generally applicable conceptual model that describes a flexible system for the trading of intellectual property through the World Wide Web. The model will be propagated through stakeholders who participate in the evolution of the model. The Propagate Conceptual Model will be comprehensive, distributed, component based developed through a process of consensus with all the stakeholders, be they creators, agents, collecting societies, distributors, publishers or end users. It will be media, asset, and channel neutral to allow for flexibility, adaptability and growth. It may be deployed as a specification, discrete application or as an API to an existing application.' - <http://www.propagate.net/project/objectives.html> (visited 15/9/98).

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(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, the types of questions we need to ask about these provisions and their national legislative implementations are:

- Can you delete from digital works personal information that facilitates surveillance?
- Can you prevent a web robot from looking for infringing artefacts?
- Can you prevent a digital work from communicating information over the Internet?

5.2. 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 it requires. In the following sections, we will take Australia and Hong Kong as examples of implementation.

From 1998 the Australian Government commenced steps to ban commercial dealings in circumvention devices and to ban removal of copyright information ('rights management information' - hereinafter 'RMI') electronically attached to copyright material' [33] . The amendments to the *Copyright Act 1968* (Cth) by the *Copyright Amendment (Digital Agenda) Act 2000* are in force since March 2001.

The Hong Kong SAR has provisions with the same intent in ss273-274 of the *Copyright Ordinance* (Cap 528).

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. Where the US has taken a different approach to protection of privacy, this is noted but not analysed in detail. The EC Directive on copyright in the Information Society, which deals with anti-circumvention and RMI issues primarily in Articles 6 and 7, was passed in May 2001[34] and is also mentioned briefly by way of comparison.

5.3. Circumvention devices - Australia

Australia's Bill drew heavily on what was then the proposed EC Directive[35], and so is of interest as a comparative 'implementation' of the Directive as well as of the WCT.

A copyright owner or exclusive licensee has a right of action (s116A(3)) against a person who makes, sells, otherwise deals in various specified ways[36] with 'a circumvention device[37] capable of

---

[33] See Commonwealth Attorney-General's Discussion Paper *The Digital Agenda* '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 Daryl Williams `Copyright and the Internet: New Government reforms' para 35, 30 April 1998, Murdoch University - <http://law.gov.au/articles/copyright_internet.html>.

[34] 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, 22.6.2001, p. 10 *et seq.*); for analysis, see Bygrave 2001 and Koelman 2000

[35] Proposed European Commission (EC) *Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society* - see Articles 6 and 7 - now Directive 2001/29/EC

circumventing, or facilitating the circumvention' of a 'technological protection measures', or a 'circumvention service'[38] with similar capability. The defendant is only liable if they knew or ought reasonably to have known that the device or service would be used for this purpose (s116A(1)). Knowledge or belief that infringement of copyright will take place is not required.

A 'technological protection measure' means (s10):

> '... 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.

Provided that such an 'access control' or 'copy control' measure does have some effect in 'inhibiting' copyright infringements, i t i s not necessary that this should be its primary purpose. It seems that any access control or copy control mechanism would at least 'inhibit' copyright infringement.

Where s116A applies, the copyright owner may obtain an injunction, damages (including additional damages) or an account of profits (s116D). There are also criminal offence where the same conditions as in s116A are satisfied, but with a higher burden of proof ('reckless' rather than 'ought reasonably to have known') and the onus of proof on the Crown (ss132(5A)-(5B)). A similar offence is created in relation to the operation of a 'circumvention service (ss132(5C)-(5D)).

The scope and effect of s116A is complex, particularly in its affect on privacy interests. In the points following I attempt to identify some of the main implications, and unresolved issues, arising from s116A.

- *Breach of copyright unnecessary* A very significant effect is that s116A gives copyright owners an enforceable right to protect access to copyright subject matter by technological measures, whether or not the attempts to circumvent those measures result in infringements of copyright.

---

[36] Section 116A(1) sets out the scope of the right:

> *116A Importation or making of circumvention device*
> (1) Subject to subsection (2), this section applies if:
> (a) a work or other subject matter is protected by effective technological protection measures; and
> (b) a person does any of the following things without the permission of the owner of the copyright in the work or other subject-matter:
> (i) makes a circumvention device capable of circumventing, or facilitating the circumvention of, those measures;
> (ii) imports any such circumvention device into Australia for a purpose of the kind referred to in section 37;
> (iii) does an act of the kind referred to in subsection 38(1) in relation to any such circumvention device; and
> (c) the person knew, or was reckless as to whether, the device would be used:
> (i) to circumvent, or facilitate the circumvention of, the effective technological protection measure; and
> (ii) for the purpose of infringing the copyright in the work or other subject-matter.

[37] s10 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 measures.

[38] s10 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 measures.

For example, it has not previously been part of the owner's exclusive rights to prevent listening to a sound recording or viewing a film in private (ie not a public performance) as these acts did not involve the making of copies. Some browsing of online works may also not involve the making of copies permanent enough to constitute an infringement.

This right to control access (irrespective of copyright breaches) is an important extension of owner's rights. The implications for user's fair dealing rights are mentioned below, but it should also be noted that even where the copyright in a work has expired and the work is in the public domain, anti-circumvention laws will still apply to protect it.

- *Users not directly liable* Actual use of a circumvention device is not proscribed, only making and dealing in such devices[39]. Nor is the act of circumvention itself covered by these provisions, though it may of course involve other forms of liability arising from the making of unauthorised copies, or criminal offences if unauthorised access to a computer system is involved. 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.

  The focus on the 'upstream' providers of circumvention devices or services, rather than their 'downstream' use (or circumvention per se) is one of the most significant limits on the scope of these provisions. However, as Koelman argues in the European context, 'too broad a prohibition on preparatory activities would render a permission to circumvent meaningless'[40] ('preparatory activities means the making and dealing with circumvention devices).

- *Broad and undefined scope of devices covered* 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 web pages 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'. If so, then the inclusion of surveillance devices as protected technology has very significant privacy implications. Similarly, a digital watermark or similar device, even if it does include details of the identity of the licensee, 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. The question Courts will have to resolve is whether 'copy control' includes deterrence or detection.

- *Unclear exemption for other commercial purposes* Circumvention devices and services are restricted to those that have 'only a limited commercially significant purpose or use ... other than the circumvention'. It would be much more clear than 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 web pages ineffective, this would seem unlikely to be a circumvention device. Similarly , if an ISP excluded all web robots from its site[41] (which may host many other content sites), and thereby excluded some which were searching for copyright-infringing content, then this

---

[39] Nevertheless, 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.

[40] Koelman 2000

[41] The Robot Exclusion Protocol is observed voluntarily by most commercial web spiders - see *A Standard for Robot Exclusion* - <http://info.webcrawler.com/mak/projects/robots/exclusion.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://info.webcrawler.com/mak/projects/robots/norobots-rfc.html> (visited 14/9/98). Site administrators have the technical capacity to exclude specific robots from their site compulsorily if they do not obey the Protocol.

would not be a breach (even if - as discussed above - such a robot was 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 used software which excluded only those robots which searched for IP infringements, it might be a different matter.

Surveillance of user's computers may be authorised A digital artefact resident on a user's PC can be designed so that it could not be accessed unless there was first an online check back to the copyright owner's database that the licence was still valid (I call this 'IP, phone home'). This could be regarded as either an 'access ... process' or 'a copy control mechanism' protected by s116A. If so, one of the most far-reaching forms of surveillance by and of digital works will be protected against circumvention - it would be illegal to assist users to circumvent such surveillance. The EC copyright Directive provsions on anti-circumvention raise similar problems of interpretation[42]

It is important to note that circumvention will be illegal irrespective of whether the personal information which is collected is used 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. Such collection may be in breach of privacy laws (see the next section), but it is arguable that anti-circumvention provisions should not provide protection for any technological measures that do not meet privacy protection standards required by legislation. This would allow technological 'self-help' against illegal technological invasiveness.

The US *Digital Millennium Copyright Act* 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'[43].

Other variants of online surveillance of users might be less clear. For example, a digital artefact that recorded its own usage even when offline, and then 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.

Fair use not recognised A piece of CPT (a 'technological protection measure') could not 'know' that the purpose for which a user wished to use a work was a 'fair use' and therefore there was no need to check whether access was licensed (because no licence is needed). The original Bill required that the defendant's actions must be for the purpose of infringing copyright, but s116A has no such restriction. As a result, various defences to infringements of copyright (such as the 'fair dealing' defences in ss40-43) do not directly provide any defence to a circumvention action. If someone makes or deals with a device (or service) to enable themselves or others to make fair uses of copyright subject matter, or to preserve the privacy of such fair uses, this will be beside the point, as knowledge of the use for circumvention is all

---

42 Bygrave 2001 says the Directive 'provides no obvious answer'.

43 See US Code Sec 1201 (i) *Protection of Personally Identifying Information* , providing protection against '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. "

that is required. Fair uses, and the privacy of fair use are not recognised by this legislation[44]. To the limited extent that defences are allowed[45], the onus of proof rests on the defendant.

In summary, the Australian legislation is limited in its effect on privacy, but may still make it illegal for people to provide protection against invasions of the privacy of 'fair use', and to protect against the secondary misuse of personal information collected via CPT.

5.4. Circumvention devices - Hong Kong

Hong Kong's anti-circumvention provisions are very different from Australia's in form, but the effect may be much the same. For clarity of comparison the same issues are considered in the same order.

- *Purpose of breaching copyright is necessary* The defendant is only liable if he 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' with works (ss 38 and 39), then this is not a breach.

- *Users not directly liable* It is not a breach of s273 to use a circumvention device *per se*. There would be a breach of the Act if an infringing copy resulted from the use, but not if the use resulted in a non-infringing copy resulted (for example, because of a fair use), or if no copy resulted. It is a breach to possess such a device, if this is 'in the course of, or in connection with, any trade or business'.

- *Liability for publishing information about circumvention* A striking feature of the Hong Kong approach is that there is liability if a person 'publishes information intended to enable or assist persons to circumvent that form of copy-protection' (s273(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, but it is not necessarily intended. An example would be a web site which provides links to overseas web sites where circumvention devices may be downloaded.

  In the USA, 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[46], and the case is being defended by the Electronic Frontier Foundation on the grounds that the anti-trafficking provisions of the *Digital Millennium Copyright Act* (DMCA) are unconstitutional because they infringe First Amendment freedom of speech rights. Similar to the USA, consideration needs to be given to whether s273(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[47] 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 s273(2)(b).

- *Broad scope of devices covered* Works are protected if they are made available 'in any form which is copy-protected', and 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'. This would not appear to cover any access control mechanisms, the circumvention of which does not involve the making of copies of a work. For example, 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, but the

---

[44] Compare Cohen 1996 Part V 'The First Amendment Case Against the Proposed Anti-Tampering Law'

[45] See s116A(2)-(4A) and (7)-(9) for various provisions exempting circumvention under some circumstances by libraries, archives, educational institutions, the Crown, law enforcement agencies etc. These exemptions do not include the 'fair dealing' defences in ss40-43.

[46] See 'Court of Appeals Asks: Is Computer Code Speech? ' EPIC Alert 8.11 at <http://www.epic.org/alert/EPIC_Alert_8.11.html > (accessed 1 October 2001)

[47] A16(3), s8 Hong Kong Bill of Rights, *Bill of Rights Ordinance* (Cap 383)

circumvention does not involve copying the work and is therefore not a breach. Where works are merely viewed, the question arises of whether the viewing involves the generation of something sufficiently permanent to constitute a 'copy' (for example, the caching of a web page). Section 23(6) makes it clear that 'copy' includes transient or incidental copies. Therefore, all access protection devices to any online or CD-ROM access to works will be covered, because access will always involve a transient copy.

- *Unclear exemption for other commercial purposes* The prohibition on dealing with devices is limited to 'any device or means specifically designed or adapted to circumvent the form of copy-protection employed'. This limitation to devices 'specifically designed' to circumvent will serve to exempt devices which have more general purposes but incidentally defeat a circumvention device.

- *Surveillance of user's computers may be protected* 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 all devices attempting to prevent unauthorised access 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.

  To the extent that online surveillance of usage is protected in Hong Kong, any protection for users against secondary usage of the information (such as marketing uses) will depend on Hong Kong's privacy laws, as the Copyright Ordinance does not itself impose any limits on use of the information collected.

- *Fair use recognised but not effectively protected* As discussed above, dealing in a circumvention device only intended to allow to allow non-infringing users would not be a breach, and nor would possessing it. Use of a device for a non-infringing purpose is not a breach, because use does not cause liability. In theory, the Hong Kong legislation is 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[48].

5.5. Rights management information - Australia

In relation to rights management information (RMI), s116B 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 s116B(3)).

Additional actions in relation to commercial dealings with copyright subject-matter from which RMI has been removed are provided in s116C, 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 s116C(3)).

Criminal offences equivalent to the actions in s116B and s116C are provided in s132(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[49], and in s132(5D) which provides related

---

[48] cf Koelman, 2000, 'Preparatory activities'

[49] s132(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

offences concerning distributing, importing and communicating artefacts where such information has been removed or altered.

'Electronic rights management information' is defined in s10 in terms very similar[50] to those in the WCT Article 12(2) and the WPPT Article 19:

> *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.

Some of the implications of the provisions for privacy are:

- *Personal information* The s10 definition of RMI does not explicitly refer to information identifying the user (the owner of the copy of the work in most cases). Bygrave and Koelman have interpreted the WTC definition as not including information identifying users such as the Purchaser ID (in the Imprimatur model)[51]. However, this interpretation is questionable, as both the WCT and Australian definitions of RMI 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 identify 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'.) 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 US *Digital Millennium Copyright Act* provisions defining 'copyright management information' imply that any information concerning users is not included[52].

- *Information transmitted is not protected* The definition of RMI (in the Australian version) only protects 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 ('IT, phone home') each time the work is used. This interpretation is also supported by the use of 'remove'. We can therefore see the RMI provisions as protecting the passive storage of RMI, but not its active dissemination. The WTC A12 requires protection to 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 A12 and 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 protected.

- *'Self-help' for privacy protection is not allowed* The Australian provision does not allow removal of RMI 'except with the permission of the owner of the copyright' whereas Article 12 of the WCT only requires prevention of removal 'without authority'. Bygrave and Koelman[53] argue that in the EU context such authority could come from what is permitted or required by

---

whether, the removal or alteration will induce, enable, facilitate or conceal an infringement of the copyright in the work or other subject-matter.

50 Though the Australian provision conjoins (a)(i) and (a) (ii) with 'and', not 'or'.

51 Bygrave and Koelman at p53

52 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'.

53 Bygrave and Koelman 1998 at p53; see also Koelman 2000

law (such as laws implementing the EU privacy Directive). However, as argued above, the Australian provisions do not seem to protect personal information as RMI (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 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 USA's DCMA.

The Australian RMI provisions therefore 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. But they may nevertheless leave users defenceless against the de facto implementation of such surveillance.

5.6. Rights management information - Hong Kong

The Hong Kong Copyright Ordinance s274 includes a definition of RMI which is essentially the same as the WCT and Australian definitions in its effect, though different in its wording[54]. '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' (s274).

The Hong Kong and Australian provisions are similar in relation to their effect on user privacy. The two references to the RMI being 'provided' by the copyright owner make it even more clear that under the Hong Kong provisions RMI protection does not extend to any data about the actual usage of works, because such data would be 'provided by' the user (even if unknowingly).

5.7. Conclusions - The cumulative effect of anti-circumvention and RMI on privacy

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

- *Can you delete from digital works personal information that facilitates surveillance?* In both Australia and Hong Kong, if the information is necessary as part of the terms of a user licence, you probably can not because it is protected RMI. Other personal information is not protected as RMI. In both jurisdictions, the removal of other personal information would not per se be actionable under the anti-circumvention provisions, but anyone dealing in devices to assist its removal could possibly be liable for circumvention, though this is not free from doubt.

- *Can 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 it is uncertain whether code to achieve this could constitute a circumvention device or service to circumvent 'copy control'.

- *Can you prevent a digital works 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

---

[54] s274(3) References in this section to rights management information means-
(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.

detection. Personal information in the process of communication does not constitute RMI because it is not 'attached' to the work at that point.

These Australian and Hong Kong examples indicate that laws facilitating technological protections of copyright could have a very substantial impact on privacy interests, but that significant issues under copyright law need to be resolved. These implementations of the WTC provisions do 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 she should still be at your place, and there are very considerable limits to what you or others can do to stop her.

6. THE EFFECTS OF PRIVACY LAWS

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 ECMS 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[55]. Hong Kong's *Personal Data (Privacy) Ordinance* (Cap 486) has been in force since 1995, and Australia's *Privacy Act 1988* (Cth) will apply to significant parts of the private sector from 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[56]. Bygrave and Koelman have each made a number of studies of the interrelationship between European privacy laws and anti-circumvention/RMI laws[57].

The United States is a special case in that the Digital *Millennium Copyright Act* contains explicit provisions limiting the operation of the anti-circumvention and RMI-protection provisions where they would infringe privacy, as mentioned above. Julie Cohen's arguments[58], prior to the enactment of that law, that laws prohibiting copyright circumvention devices diminish 'the right to read anonymously' and may breach the guarantees of freedom of speech and privacy in the US Constitution are of limited relevance as legal arguments to countries such as Australia which do not have such constitutional guarantees, but potentially more valuable in Hong Kong. Most European and some other countries are more willing than the USA to protect privacy by general information privacy legislation. In many other countries, there is likely to be less reluctance to interfere in 'private orderings' of transactional relationships concerning intellectual property by legislation, for example by compulsory licensing schemes. Even in the USA, compulsory terms in such contractual relationships are not so unusual[59].

6.1. Is ECMS 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 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 (s 6). Hong Kong's definition is similar[60].

---

55 New Zealand and Canada are the other significant examples.

56 Directive 95/46/EC of the European Parliament and of the Council of 24 October 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, 23.11.1995, p. 31 *et seq.*)

57 See Bygrave and Koelman, 1998, particularly Chapter 2; Koelman, 2000; and Bygrave 2001.

58 Cohen 1996

59 Terry Fisher stresses that compulsory terms in contracts are not at all unusual in the USA., and proposes a set of such compulsory contractual terms for contracts concerning intellectual property rights: see Fisher 1998

60 Section 2 defines 'personal data':

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 email addresses would constitute personal information would usually be a question of fact in a particular case[61]. Bygrave and Koelman also though this was uncertain[62].

In the ECMS context, there may be many doubtful situations. For example, if a web spider merely collects the ID number of a licensed digital work, but it is possible for that ID 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 web page, the combined information can still be 'personal information', but this will depend on the wording of particular legislative provisions[63].

However, these types of definitions may miss the real point of many cyberspace interactions. If an ECMS can determine that a copy of a digital work it has located on the net 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 suable, 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 valuable to market other digital works to that individual, and there is access to an email 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.

6.2. Anonymity and pseudonymity as privacy rights

It is possible for many aspects of ECMS 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 ECMS are in direct conflict with rights of anonymity and pseudonymity. Issues of purpose specification will be crucial. ECMS intermediaries can use pseudonymity in order to maintaining 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 ECMS that protect privacy[64].

In Australia's privacy law, National Privacy Principle 8 'Anonymity' (NPP 8) requires 'Wherever 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[65] and

---

"'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 ' (s2)

61 Greenleaf 1996

62 Bygrave and Koelman at p14

63 See Greenleaf 1998, Part F 'Stopping Searching - Robot Exclusion Standards' for discussion.

64 See for example Greenleaf 1999a; Weinberg 2000,

65 Its local 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* - at <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* (<http://www.privacy.gov.au/news/p6_4_1.html> (visited 14/9/98)) included Principle 8 'Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when

is not required by the European data protection Directive[66]. 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.

There is no explicit equivalent in the Hong Kong Ordinance. It would be difficult to read a requirement of pseudonymity or anonymity into the scattered words of Data Protection Principle (DPP) 1[67] 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*[68] , 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.'

It is this design requirement that makes the specific requirement on service providers to provide anonymous and pseudonymous uses of teleservices 'to the extent technically feasible and reasonable'[69] a meaningful requirement, 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 the Internet[70] which show a clear preference for maximising anonymity in

---

entering transactions'. The Victorian State Government has included this Principle in its *Data Protection Bill 1999* (with 'should' changed to 'must').

66 see Bygrave 2001 for discussion

67 Schedule 1

68 Article 2 of the *Information and Communications Services Act* of 1997 - see references above; It is an early legislative example of 'systemic data protection' ('Systemdatenschutz').

69 '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.'

70 Article 29 Committee 1997a; 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.

...

Internet transactions, subject to balancing this with other rights. [71]. In 1999 the International Working Group on Data Protection in Telecommunications, drawn from data protection agencies worldwide, specifically recommended the development of ECMS 'which allow for anonymous or pseudonymous transactions'[72].

6.3. 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). The following 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). It remains to be seen whether CPT operators can avoid this limitation simply by giving notice of intention to use personal information for marketing purposes as well as for copyright protection. It could be argued that the statutory protection in relation to circumvention devices and RMI means that the only those functions should be allowed as purposes of collection, but this is speculative.

- Notice of collection, use and disclosure practices must be give 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. DPP 1 has similar provisions, but only in relation to collection directly from the data subject. These notice requirements will cause the greatest difficulties for some CPT operators, as mentioned below.

Many aspects of data collection by ECMS 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)[73].

More contentious forms of collection of personal information are likely to arise because of the surveillance aspects of ECMS. If a monitoring service provider (MSP) uses a web spider solely for the purpose of collecting rights management information (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 may 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

---

- 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.

[71] For the importance of this distinction, see Clarke 1999 and Smith and Clarke 1999

[72] International Working Group on Data Protection in Telecommunications, 1999

[73] For discussion, see Bygrave and Koelman at p16-, also p 27

will be no consent to collection and no contract, so justification for collection may be more difficult to provide.

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 (hereinafter 'the Article 29 Committee') made recommendations in February 1999 concerning automated processing which is unknown to the user[74] which are relevant to the collection of data by ECMS and CPT. 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'. All five recommendations are relevant (I have substituted 'digital works' for 'software' in discussing them):

- *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.
- 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 whenever a cookie is to be received, stored or sent, and in generally understandable language. Germany's *Teleservices Data Protection Act* already provides such a requirement of notification before processing commences (s3(5)).
- 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[75].
- Users should be able to 'freely decide' about the processing of their personal data, and modify what items are processed (Recommendation 4).
- 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.

6.4. Limits on use and disclosure

The finality principle has significant implications for the operation of ECMS. NPP 2 in the Australian Act prevents personal information collected by copyright-protective technologies from being used or disclosed for any secondary purpose unless the secondary use is:

- a directly related use which would be reasonably expected; or
- with consent; or
- 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 s34 (direct marketing) have a similar effect.

---

[74] Article 29 Committee 1999a

[75] See Greenleaf 1998

Secondary uses, particularly marketing uses, are analysed by Bygrave and Koelman[76], who note a number of European provisions which could have a significant effect on ECMS operations:

- *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 personal information. If a CPT terminated the suability 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.

- *Aggregation of different services* 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 (s4). Such a restriction would significantly limit the secondary uses of ECMS information. There is no direct equivalent in the Australian or Hong Kong legislation.

6.5. Data export prohibitions, extra-territorial operation, and conflicts

ECMS 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.

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 the prohibited jurisdiction, and whether any exemption allowing this applies. Depending on the type of CPT used, there may be

As is well known, the EU data protection Directive[77] requires European privacy laws to include data export prohibitions. In many instances the exceptions in Article 26 of the EU privacy Directive will apply[78], 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 data exports to countries without privacy laws of similar effect to the Australian law. Exceptions are made for transfers with consent, pursuant to a contract or pre-contractual negotiation, for the individual's presumed benefits, transfers to jurisdiction offering similar protection, and transfers 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 (s33) is one of the few sections not yet in operation. Its provision are very similar to the Australian NPP 9, but slightly stricter.

7. RESTORING THE BALANCE - DO WE NEED PROTECTION FROM COPYRIGHT?

7.1. What privacy protections are needed? - a beta list

Large-scale implementations of CPT and ECMS are still in a sufficiently early stage that it is premature to offer more than a speculative list of what protections may be needed as the technologies and

---

[76] Bygrave and Koelman p23

[77] Directive 95/46/EC of the European Parliament and of the Council of 24 October 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, 23.11.1995, p. 31 *et seq.*)

[78] See Bygrave and Koelman pgs 29-31 for detailed analysis.

business models mature. It is also too early to be certain how serious the potential risks will turn out to be, as Bygrave warns[79]:

> 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.

At the same time, legislation is now giving pro-active protection to CPT and ECMS, 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.

Here is such a beta list of the changes that may be needed in jurisdictions such as Australia and Hong Kong, offered to provoke further discussion:

- 'Anti-circumvention' copyright protections should be limited strictly to the scope of the exclusive rights of a copyright owner, and should not include subject matter which is in the public domain, subject to fair dealing defences, or merely constitutes access without breach of an exclusive right.
- It should be a defence 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 copyright.
- Definitions of 'personal information' and the like should be strengthened to apply to more cyberspace transactions affecting individuals, possibly including any transactions allowing interaction with an individual on a personalised basis.
- 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'). Blocking or removal of such information should be an exception to copyright laws and to anti-circumvention laws.
- Protections of rights management information (RMI) should not require individuals to submit to active online surveillance and reporting by digital works on their computers.
- Users should be given positive legal authority to prevent collection of personal information (or remove the information) in breach of privacy laws. Blocking or removal of such information should be an exception to copyright laws and to anti-circumvention laws.
- System designers should be required to maximise the use of CPT which allows anonymous transactions (balanced against problems of unfair contract enforcement) where commercial objectives can be met without identification, and allows pseudonymity where it is necessary for transactions to be identifiable in order for commercial goals to be met.
- Default configurations of digital works should not enable surveillance capacities but (if the user does have a choice) should require the user to 'opt in' before surveillance takes place..

7.2. What can privacy officials do?

Data protection and privacy Commissioners need to take steps in their own jurisdictions, if they have not already done so, including:

- Encouraging developers and vendors of CPT and ECMS in their own jurisdiction to develop and publish privacy policies.

---

[79] Bygrave 2001

- Enforcing, where appropriate, data protection laws against the local implementations of CPT and ECMS, particularly in relation to the provision of anonymity / pseudonymity options and excessive collection of information.

- Taking an active role in local debates on legislation concerning circumvention devices and RMI.

- Engaging 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 ECMS. Consumer organisations are starting to express concern[80] and should be included in any dialogues.

8. REFERENCES

- Article 29 Committee (1999a) 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 February 1999) - <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp17en.htm>

- Article 29 Committee (1997a) The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data *Recommendation 3/97 Anonymity on the Internet* (3 December 1997) - at <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp6en.htm>

- John Perry Barlow (1993) 'Selling Wine Without Bottles: The Economy of Mind on the Global Net' Wired 2.03 (1993) at 86 - at <http://www.eff.org/pub/Publications/John_Perry_Barlow/HTML/idea_economy_article.html> (visited 19/10/98).

- Lee Bygrave and Kamiel Koelman (1998) *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems* Institute for Information Law, Amsterdam, June 1998 at p5 (Report commissioned for the Imprimatur project) - <http://www.imprimatur.alcs.co.uk/IMP_FTP/privreportdef.pdf>.

- Lee Bygrave (2001) 'The technologisation of copyright: Implications for privacy and related interests'; draft presented to 'Data Protection and Intellectual Property on the Internet' conference, Berllin 27 August 2001; to be published in issue 24(1) *European Intellectual Property Review*

- Roger Clarke (1999) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' *IFIP User Identification & Privacy Protection Conference*, Stockholm, June 1999 - at <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html>

- Roger Clarke and Gillian Dempsey (1999) 'Electronic Trading in Copyright Objects and Its Implications for Universities', Australian EDUCAUSE'99 Conference, Sydney, 18-21 April 1999 - at <http://www.anu.edu.au/people/Roger.Clarke/EC/ETCU.html> (visited 19/6/1999)

- Julie Cohen (1997) "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them," 12 Berkeley Tech. L.J. 161 (1997) - at <http://www.law.berkeley.edu/journals/btlj/articles/12-1/cohen.html>

- Julie Cohen (1996) "A Right to Read Anonymously: A Closer Look at 'copyright management' in Cyberspace", 28 Conn. L. Rev. 981 (1996) - at <http://cyber.law.harvard.edu/property/alternative/Cohen.html>

- Brad Cox (1994) 'Superdistribution' Wired Archive | 2.09 - Sep 1994 - at <http://www.wired.com/wired/archive/2.09/superdis.htm>

---

[80] Transatlantic Consumer Dialogue (TACD) Meeting 23-24 April 1999, Brussels Recommendations on Electronic Commerce Recommendation 2.: 'Privacy. There are important conflicts between privacy and certain technologies that protect copyrighted materials. Privacy is a social good. Society should avoid mechanisms to protect copyright that are unreasonable intrusions on personal privacy, particularly when less intrusive mechanisms are technologically feasible.' (see <http://www.tacd.org/>)

- Coalition for Networked Information (1994) Proceedings: Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment - at <http://www.cni.org/docs/ima.ip-workshop/>

- William W Fisher III 'Property and contracts on the internet' (draft paper), presented at the *1998 Internet Law Symposium* Science & Technology Law Center, Taiwan, June 1998 - at <http://eon.law.harvard.edu/property/alternative/98fish.html>

- Daniel J Gervais (1998) 'Electronic Rights Management and Digital Identifier Systems' - *The Journal of Electronic Publishing* Volume 4, Issue 2 March 1998 - at <http://www.press.umich.edu/jep/04-03/gervais.html> (visited 22/6/99)

- Graham Greenleaf (199a) '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/conference.html> (visited 2 October 2001); HTML version available at <http://austlii.edu.au/~graham/publications/ip_privacy/> (visited 2 October 2001)

- Graham Greenleaf (1999) "Victoria's draft Data Protection Bill - The new model Bill?" 5 *Privacy Law & Policy Reporter* 36 - at <http://www2.austlii.edu.au/~graham/cyberspace_law/Vic_Bill.html>

- Graham Greenleaf (1998) 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) University of New South Wales Law Journal Volume 21, Number 2 'Electronic Commerce: Legal Issues For The Information Age', November 1998 - at <http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/greenleaf.html>

- Graham Greenleaf (1996) 'Privacy principles -- irrelevant to cyberspace?' (1996) 3 PLPR 114 - at <http://www.austlii.edu.au//au/other/plpr/vol3No06/v03n06d.html>

- International Federation Of Reproduction Rights Organizations (IFRRO), Committee On New Technologies, *Digital Rights Management Technologies* - was, but no longer at <http://www.ncri.com/articles/rights_management/>

- Kevin Kelly 'New Rules for the New Economy' WIRED archive 5.09 September 1997 - http://www.wired.com/wired/5.09/newrules.html (visited 16/6/1999)

- Kamiel Koelman (2000) 'A hard nut to crack: The protection of technological measures' (2000) *European Intellectual Property Review*, 227-288; draft available at <http://www.ivir.nl/publications/koelman/hardnut.html> (visited 2 October 2001)

- Robert Lemos 'Intel to electronically ID chips' ZDNet News 21 January 1999 - at <http://www.zdnet.com/zdnn/stories/news/0,4586,2189721,00.html>

- L Lessig 'The Law Of The Horse: What Cyberlaw Might Teach' - <http://cyber.law.harvard.edu/works/lessig/law_horse.pdf> (June 11 1998 draft - visited 14/9/98) and <http://stlr.stanford.edu/STLR/Working_Papers/97_Lessig_1/index.htm> (Stanford Technology Law Review Working Papers 1997 draft)

- Charles C. Mann (1998) "Who Will Own Your Next Good Idea?" Part II, The Atlantic Monthly, September 1998 - at <http://www.theatlantic.com/issues/98sep/copy2.htm>

- Anita Smith and Roger Clarke (1999) 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>

- Mark Stefik (1997) 'Shifting The Possible: How Trusted Systems And Digital Property Rights Challenge Us To Rethink Digital Publishing' *Berkeley Technology Law Journal*, 12, 1 (Spring 1997) - at http://www.law.berkeley.edu/journals/btlj/articles/12-1/stefik.html (visited 19/6/1999)

- Jonathan Weinberg (2000) "Hardware-Based ID, Rights Management, and Trusted Systems'; available at <http://www.law.wayne.edu/weinberg/newstanford.PDF> visited 2/10/2001)

- The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data - see 'Article 29 Committee'

- International Working Group on Data Protection in Telecommunications *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> (visited 2/10/2001)