Chapter 2

Whose rights need to be managed?

T. J. Laidler

© – the 'Copyright Bundle'

One small symbol makes it all seem so simple, as do modern legal structures that go under the deceptively straightforward, generic name, *copyright*. But, anyone who has attempted to grapple with the complexity of licensing and registration rules, systems and bodies that oversee the ways in which we access, enjoy and use the creative work of others in our society knows it is not quite that easy. The *bundle* of rights to which copyright refers has developed dynamically in parallel with emerging technologies of publication and distribution. This development has been occurring since the invention of the printing press when, perhaps, it referred to the seemingly *simple* authority given to a printer to make copies of an author's book.

However, the complexity is manifest from the beginning in the way different legal systems have dealt with the matter. Civil law (or codified) systems (such as the French, inspired later no doubt by libertarian, revolutionary principles) have based their jurisprudence on the principle that creativity springs from the personality of the creator, and see the bundle of rights in the context of a more general theory of human rights as 'la plus sacrée, la plus personelle de toutes les propriétés' (the most sacred and personal of all property: Le Chapelier, 1791, cited in Stewart, 1989). It is hardly surprising, then, that doctrines of the moral rights of the author grew first in this tradition.

Common law jurisdictions (based on evolving case law, such as our own or that in the US) start from a more mechanical premise that the new printing technologies allowed easier reproduction. Since the English *Statute of Queen Anne*, 1709, this has expression in the need to protect booksellers' economic interests. Not surprisingly either, these jurisdictions had less difficulty in dealing with the notion of corporate ownership of intellectual property because 'whoever takes the initiative in creating the material and makes the investment to produce it and market it, taking the financial risks that such activities involve, should be allowed to reap the benefit' (Stewart, p.8).

Current international law on copyright (and neighbouring rights, such as those applying to film and sound recordings in jurisdictions where, strictly, copyright is reserved for literary works) combines these two approaches. The *Berne Convention for the Protection of Literary and Artistic Works* (1886) adopted in the *World Intellectual Property Organization (WIPO) Treaty* (1996) specifies the ten rights that treaty nations accept as basic to regulating the way their communities deal with the creative expression and publication of ideas:

- the **moral rights** of the author to determine when where or whether a work will be published, to have authorship attributed, and to safeguard reputation by preserving the integrity of their work;

- the **reproduction right** of the author to authorise the reproduction of their work in any manner or form (which was not formally incorporated into the Convention as article 9(1) until 1967, perhaps because the concept of **copy**right was seen as self-defining);
- the **translation right** ;
- the **public performance right** which covers not only live performance of dramatic and musical works but other modes of presentation;
- the **public recitation right** which is similar to the public performance right but which applies to literary works;
- the **broadcasting right** originally in respect of radio and television, but increasingly, in so-called *technology neutral* regulatory regimes, other forms of one to many dissemination, for example web publishing;
- the **right of adaptation** conferring on an author the exclusive right to authorise any alteration or arrangement of their work;
- the **recording right** from which most compulsory licence systems derive their justification;
- the **film right** allowing authors of pre-existing works to authorise screen adaptations and to benefit from them, and film makers and owners the other rights specified here, and
- the '**droit de suite**' (right of 'follow up') allowing creators of works other than books a similar prerogative to authors to gain profit from sales of their painting, statue, engraving etc. subsequent to the original sale.

The 1996 *WIPO Treaty* adds an eleventh right:

- the **right of rental** conferring on creators the right to authorize and gain benefit from the commercial rental to the public of the originals or copies of their works.

In all this, the Treaty makes it clear that while:

> Recognizing the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works, … [and] the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information … copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such (Preamble and article 2).

In this modern formulation, we can see one of the tensions at the heart of the implementation of copyright systems that has emerged again and again: rights protection regimes for creative have to balance a variety of objectives.

A balance of rights

The law of copyright exists to balance two principles important to the functioning of a learning society. These principles are enshrined at the heart of the *UN Universal Declaration on Human Rights*:

> Article 27.
>
> (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.
>
> (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

This is no new concept: as that most conservative English jurist, Lord Chief Justice Ellenborough (of 'the greater the truth the greater the libel' fame) put it early in the nineteenth century, '… the state must indeed endeavour to secure for authors the enjoyment of their copyrights but not to the extent that doing so places 'manacles upon science'' (cited in Loren, 1997). Similar sentiments have been echoed in other jurisdictions, such as the US, where the Constitution enshrines a public good purpose for copyright:

> The primary objective of copyright is not to reward the labour of authors, but '[t]o promote the Progress of Science and useful Arts.' To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work. This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art. (Justice Sandra Day O'Connor [Feist Publications, Inc. v. Rural Telephone Service Co., 499 US 340, 349(1991)])

The notion that the creators of the images, forms and expressions that encapsulate ideas are entitled to the rewards of their work, and that others should not unfairly benefit from their work, accords so well with our common ethical understandings that there can be little doubt that this aspect of the legal regime of copyright will survive. Indeed, it may be true that the present state of copyright law in Australia, for example, better acknowledges the community's duties to the creators of original ideas and is less concerned about the protection of distribution mechanisms than at many other stages of its evolutionary history (Laidler, 2001).

For example, the Australian Parliament in late 2000 passed changes to the *Copyright Act* 1968 to protect further some of the traditional 'moral rights' of authors or creators in their work, specifically:

- **the right of attribution**: the author's right to be known to the public as the creator of the work and not to have works falsely attributed to them.
- **the right of integrity**: the right to object to distortions and mutilations of the author's work in such a way that would prejudicially affect the author's honour or reputation.

The Australian Act did not include two other categories of 'moral right' found in the so-called 'code' jurisdictions, namely:

- **the right of disclosure**: the author's right to determine if and when a work is to be divulged to the public;
- **the right of withdrawal**: the right to withdraw a work from the public, if the author wishes.

Nonetheless, the amended Act provided broad discretionary remedies to Australian courts where they find moral rights have been infringed and illustrates that, to some

extent, it is the very evolution of new digital communication technologies (e.g. photo and audio editing software available on desktop PCs) coupled with the corporatization of creative endeavour that has focussed attention even more sharply on the need to protect authors and artists in these ways. After five hundred and fifty odd years of mass publication, authors' rights might seem to be in the ascendancy even in common law jurisdictions!

Rights askew?

However, the understanding that there is a social good to be preserved in the free flow of ideas may not have been so fortunate. This understanding has always been protected in traditional copyright law by, among other things, a doctrine of fair use or dealing and the fact that when copyright ends, works become part of the public domain. However recent legislative interventions, for example the US *Digital Millennium Copyright Act of 1998*, have sought not only to restrict or eliminate fair use insofar as digital media are involved, but also to extend the duration of copyright to up to more than 150 years, and to prevent activity designed to circumvent protection technologies even where no infringement of copyright takes place.

There is a growing movement that reflects a concern that both the commercialization of knowledge that has occurred over the past 15 or so years, and the focus on *digital rights management* synchronous with, and made possible by, new information and communications technologies (ICTs) may have pushed the balance too far against the broader interests of the free flow of information in a civilized, democratic society.

As of 15 August 2001, more than 26 000 scientists from 170 countries had signed a petition asking that the preservation of a 'public domain' of important scientific information receive equal attention to the protection of intellectual property rights:

> We recognize that the publishers of our scientific journals have a legitimate right to a fair financial return for their role in scientific communication. We believe, however, that the permanent, archival record of scientific research and ideas should neither be owned nor controlled by publishers, but should belong to the public, and should be freely available through an international online public library.
> (http://www.publiclibraryofscience.org/plosLetter.htm, viewed 15 August 2001)

The Berkman Centre for Internet and Society is the home of a more general counter-copyright movement that seeks to apply understandings generated in the 'open source' software movement (http://www.fsf.org/licenses/gpl.txt, viewed 15 August 2001) to more general realms of endeavour such as text publishing:

> The idea surrounding the counter-copyright campaign is fairly easy to understand. If you place the [cc] icon at the end of your work, you signal to others that you are allowing them to use, modify, edit, adapt and redistribute the work that you created. The counter-copyright is not a replacement for an actual copyright, rather it is a signal that you as the creator are willing to share your work. The counter-copyright strips away the exclusivity that a copyright provides and allows others to use your work as a source or a foundation for their own creative ideas.
> (http://cyber.law.harvard.edu/cc, viewed 15 August 2001)

These issues are not just theoretical, as illustrated by the recent case of Adobe 'hacker' Dmitry Sklyarov, who spent 21 days in gaol before bail for allegedly violating the *Digital Millennium Copyright Act* by creating a decryption tool that can be used to facilitate copyright violations. The Russian software engineer was arrested by FBI agents in July 2001 after delivering a paper on e-book security at the Def Con hackers' convention in which he admitted circumventing the security of an Adobe Systems e-book program (http://uk.news.yahoo.com/010807/101/c0mcq.html, viewed 12 August 2001).

The Electronic Frontiers Foundation took Sklyarov's case up and, as well as gaining widespread popular press, it quickly became a *cause celebre* among movements concerned at what they see as an imbalance in the development of legal regimes designed to protect technologies that do not allow sufficient free flow of valuable social information (http://www.eff.org/alerts/20010720_eff_sklyarov_alert.html, viewed 12 August 2001).

An example of judicial intervention aimed at redressing the imbalance that some would see emerging can be found in the US Supreme Court's decision in Feist vs. Rural Telephone (499 US 340 [1991]). The decision surprised many, but was entirely consistent with the principles later made explicit in the *WIPO Treaty* (1996):

> Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation (article 5).

The judgment drew attention again to the need to strike this balance of rights. The Court decided that a telephone book, despite the undeniable cost and labour required to assemble it, did not represent a form of expression of sufficient creativity or originality to merit copyright protection. The decision suggests that creative organization is what is to be protected by copyright, not simply information itself.

However, the relational databases that underlie so many Internet technologies avoid organizing material in their fundamental architecture in order to make retrieval as efficient as possible. The decision in Feist implies that databases cannot be protected at all unless they represent some creative new taxonomy of information – which is why database vendors are so keen on claiming new forms of protection for their products.

Technologies and rights protection

Moreover, new digital information technologies are not just *works* to which copyright might apply; increasingly they are part of the *architecture* of copyright protection.

Lessig (1998) has suggested that four sorts of constraints regulate behaviour in the real world:

- Law: which regulates by sanctions imposed *ex post factum*;
- Social norms: which set constraints through the understandings and expectations of just about everyone within a particular community;
- The market: which regulates by price to set boundaries on opportunities; and

- What he calls ‘architecture’: where the very nature of what is being regulated sets limits on our actions in relation to it.

In this context, technology has always contributed to the complex social structures by which we have sought to balance the rights of creators, the rights of those who take commercial risk in the dissemination of creative works and ideas, and the rights of the entire community to benefit from the enjoyment of art and its critique of our societies, and the free flow of knowledge and information. The printing press itself, part of the *architecture* of book making, was once a natural copyright protection technology. Without a press, one needed a school of monks to copy more than a fragment of a text! The inventors of the presses, those who fed and primed them, were often at once the custodians of the protection technologies and the great champions of the wide dissemination of ideas, much to the chagrin of sovereign powers who sought to control the dangerous flow of new ideas (Kaplan, 1967).

And we forget that the *architecture* of broadcast technology is barely 80 years old and of publicly available sound recording, 50 years old. Until that time, the *law* which protected the performance, recording and broadcast rights of creators and authors was pre-eminently the domain only of individuals and more often companies that could afford the technologies of reproduction. Most copyright was protected by the *market* and *architecture*. The Australian experience of ‘hackers’ with their crystal radio sets breaking the ‘fixed tuned’ wireless receiver ‘encryption technology’ of the vertically integrated Marconi broadcast monopoly and its licence payment system demonstrated the problems which emerge when technological solutions and *social norms* conflict. In that case*, law*, *market* and *architecture* adjusted to give wider community access to sought after information and services (cf.: e.g. Inglis, 1983, pp. 6-10).

Herein lies one of the dilemmas that faces digital rights management today: where the combination of law, social norms, market forces and architecture protects well the rights of authors and dissemination entrepreneurs in the vast majority of cases, and most especially if it prevents gross, unfair economic exploitation, what social and economic value is there in designing increasingly complex technological solutions and legal systems to ensure near perfect compliance? What opportunity costs, social and financial, are involved in *copyproof copyright*?

The social value of unenforced copyright?

There is an old legal adage, *de minimis non curat lex (or praetor)* or “the law does not concern itself with trifles” (Martin, 1997). While most of the older case law applying it involves commodity and real estate measurement, it might be time to dust it off in a new context. It has recently been applied to general trade treaties (*Alcan Aluminum Corp. v. U.S.*, 165 F.3d 898 Fed. Cir. 1999) and to environment protection law (*Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Matter*, International Maritime Organization, Geneva, 1972). Applied here, it would suggest that there are parts of the copyright regime where the economic value of a breach or the personal wrong done to a creator of a work are not such as to merit the legal and social burden of pursuing them.

In some ways, the general legal principles applied in estimating what is fair dealing for the purposes of copyright are already an application of the doctrine. The Australian *Copyright Act* 1968, for example, provides that courts should take account of both "the effect of the dealing upon the potential market for, or value of, the work or adaptation" and "in a case where part only of the work or adaptation is reproduced—the amount and substantiality of the part copied taken in relation to the whole work or adaptation" (Section 40 (2)).

Copyright and its protection regime in the physical environment have never sought to capture, register and take commercial benefit from every use of every part of every creative work ever produced. Regardless of whether technology makes such capture possible, the question of what real economic or social benefit there is to be had in doing so is the moot point.

One does not have to share the near anarchistic view of John Perry Barlow, a former lyricist for the Grateful Dead, and co-founder of the Electronic Frontier Foundation, to believe that, if a principle of proportionality such as that enshrined in the *de minimis* doctrine is applied, the new communications technologies can be the mechanism for righting the imbalance that might occur if governments seek to protect creators' and publishers' rights too rigorously. In his *Declaration of the Independence of Cyberspace* (1996) Barlow wrote:

> Governments of the industrial world, you weary giants of flesh and steel, on behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. Cyberspace does not lie within your borders.

Surely, a "global *social* space" is one in which the work of creators is morally valued and the risk of those who publish acknowledged, regardless of the threat of enforcement? And just as surely, any notion of liberty that does not see me as having a duty to allow the liberty of others is a very circumscribed view of freedom. Nevertheless, even in an online environment less romanticized than the one Barlow speaks of, it is clear that the new technologies and services could be media for the more extensive free expression of innovative ideas to wider and more participative audiences.

Nor does one need to share the neo-Marxist analysis of McKenzie Wark (*The Hacker Manifesto 2.0*, 2001) who sees "hackers" as an innovative "class" and "hacking" itself as almost synonymous with the process of creative production, to understand that, if intellectual property protection systems are so extreme as to offend basic social norms about fair dealing in information, they will invite circumvention.

Unless, of course, those who seek to make every post an economic winner have their way! At this other end of the scale, are those who exaggerate the risks if technologically foolproof solutions to managing rights protection are not implemented. While the law may not concern itself with trifles, perhaps emerging technologies can:

> … in the non-digital environment, securing copyright "permissions" is a complicated, time-consuming and often unsatisfactory process. Owners and publishers are already often unable to

> cope with the volume of low-value permissions requests made in conventional ways. In the digital environment … without automation, all but the most valuable permissions will become impossible to administer (Rust & Bide, 2000).

Keeping the balance – socially and economically

What is it, then, that leads to such efforts to use technologies to tighten or even "perfect" copyright protection and enforcement regimes?

In the most pejorative analysis, it could be merely one more step in what Ivan Illich observed over a quarter of a century ago as an all-pervasive thrust towards the commodification of human activity, especially

> objective knowledge [which] is viewed as a commodity which can be refined, constantly improved, accumulated and fed into a process, now called "decision-making." (1973, p.86).

Making all knowledge an identifiable, tradeable commodity, and coupling the technology that enables that with others that enable "micro-charges" allows a new domain of commerce to be born. In a reductionist social philosophy that sees market forces as the most parsimonious arbiter of the socially good, and that has *homo economicus* motivated by wealth generation as its dominant anthropology, this approach could gain some credence.

In the best analysis, any such enterprise is probably a misunderstanding of the complex social system that copyright is: a failure to understand the dynamic process well characterized by Barlow as the interaction between law, market, social norms and architecture. At its roots, such a misunderstanding most probably does not understand the balance of rights that copyright has always sought to make, nor the social damage that could be done if endeavours to protect the rights of creators and those who disseminate their works actually impeded the growth of learning communities.

That the learning community might, in fact, be globalizing aided by new information and communication technologies is no less reason for protecting its growth. It may, indeed, be reason for offering it more scope. Of all times in recent history, this may be the most opportune for tilting the balance in favour of the mechanisms that advance freer information flow if the socio-economic advantages touted for globalization are to be achieved. The concerns of those who protest at Davros, in Melbourne and Genoa (cf: http://www.theage.com.au/issues/economicforum/index.html) focus on the concentration of information and resources in the hands of the few away from the many, and on what is perceived as economic growth oblivious to cultural and personal choice. To the extent that the Internet and its client technologies make more inclusive communication and the wider propagation of expansive ideas possible, would it not be wise to take every opportunity to open or leave open this door? There is a social cost to closure.

Moreover, allowing for, even encouraging, growth in the learning community and its information exchange systems has a sound economic rationale.

One way to facilitate wealth generation is to "deepen" the market, to drive even further down the supply chain opportunities to create value and to derive income from smaller and smaller transactions. Another is to "broaden" the market, to allow new people and groups opportunities to participate and see value in the exchange of ideas. This broader

market would not only introduce new buyers, but also new products: the new technologies that make new scales of production efficient, content previously the domain of a few that might enrich many, the new intermediary processes and systems that must emerge for dealing in the new environment.

Those who read books, appreciate art, enjoy drama and music and the like are surely more than just consumers from whom every last drop of value must be extracted. They are Chapter 4's "smart yet hamstrung consumers and readers". They are also creative people themselves wanting to originate and adapt, learn and teach, grow and participate, buy and sell, wonder and worry, influence and absorb. They are citizens, competitors, collaborators, listeners, viewers, producers and manufacturers. In short, they are moral agents, trying to do what is ethically good at the heart of complex networks of relationship with others. They have a right to expect community knowledge management systems no less able to serve them in the complexity of their aspirations than those upon which they build.

Chapter 3

Digital Rights Management Systems (DRMSs)

T. J. Laidler

> ***Digital Rights Management (DRM). (n.)*** The definition, protection, or enforcement of rights pertaining to content produced, delivered or accessed electronically (Open eBook Forum, 2000).

The bundle of rights that are the meat of copyright law allows an owner of a work to confer rights to sell, trade, make copies, or other transactions. Digital rights management (DRM) technology supports the definition and conferral of copyright to digital works, and protects the authenticity, integrity and quality of those works for those on whom rights are conferred. DRM processes also need to protect the privacy of those on whom rights are conferred, and to maintain them in dynamic balance with the needs of learning societies for the free flow of information about culture, politics, science and the arts, and the rights of individuals and groups to join the public discourse about these vital social undertakings.

In some ways, DRM is a misnomer, then: there is no new set of rights called "digital rights". They are the same old bundle of rights in and to creative content that copyright regimes have known for a long time. What has changed is way we are able to present content, and consequentially and perhaps most importantly, the storage, management and distribution mechanisms for that content, most notably the Internet.

There is considerable interest and activity in the area of DRM for the delivery of various types of digital objects due to this growth of the Internet, both in its reach and bandwidth. As Robert Bolick from McGraw-Hill Professional has noted, citing the American Association of Publishers:

> Digital rights management (DRM), the technologies, tools and processes that protect intellectual property during digital content commerce, is a vital building block of the emerging electronic book (ebook) market. DRM creates an essential foundation of trust between authors and consumers that is a prerequisite for robust market development (2000).

While many DRMSs have had a security and protection focus, Renato Ianella rightly draws attention to the broader context in which the issue of rights management in a digital environment must be considered:

> DRM is broader and includes description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationship (2001).

The use of the Internet to distribute rights-managed digital objects has necessitated the introduction of new technologies to engineer protection into digital products themselves, and to look again at the very heart of the Internet Protocol (IP) architecture to ensure that its structure is able to allow the reasonably effective protection of copyright.

The open standards consortium structure, used reasonably successfully in the development of Internet protocols so far (for example, for Internet domain names [IANA & ICANN] and the world wide web standards [W3C]) has been invoked to deal with Internet digital rights management (IDRM).

The open standards approach is seen as a way of ensuring that DRMSs protect the balance of rights needed in managing intellectual property.

> …This is important so as not to upset the balance between the different interests inherent in copyright, especially with regards to the free flow of information. Open standards regarding DRMS are to be favoured, since these normally implies large consultation by interested parties and reduces the risk of the measures being anti-competitive in nature. Furthermore open standards and common platforms increase the possibility to create seamless environments and enhance interoperability (Still, 2001).

Related working groups are investigating digital object identification (DOI) systems, and there is considerable effort going into the taxonomies and metadata standards and registration agencies that will be needed to allow efficient management of DRM systems within the Internet protocols (as examples, <indecs>, the Dublin Core Metadata Initiative (DCMI) [for detail see below] and the Australian copyright registration agency, CAL).

International legal systems have already begun to adapt to the need for these new technologies, with WIPO Treaty participants agreeing to 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 restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law (article 11).

The US *Digital Millennium Copyright Act* and changes to the Australian *Copyright Act* mentioned are examples of the incorporation of this commitment into domestic law.

Whether to date this combination of technological solutions and legal regimes has achieved the requisite balance of rights and duties is the substance of Chapter 1. There are strong proponents of the view that it has not:

> You don't have to be a pirate to be concerned about this trend, especially when one adds to it the changes that cyberspace is now inducing. For in addition to these protections granted by law, code writers for copyright holders have built technologies that supplement the law. This code adds to the control that copyright holders have over the use of their content. Using this code, copyright holders can now direct, for example, how often a book can be read, or by whom; they can control whether or what parts can be copied, or on what machine the book can be read. This additional control is facilitated through software – and this software is now backed by the force of law. The anti-circumvention provision of the Digital Millennium Copyright Act makes it an offence to write code to interfere with this use-controlling code, regardless of whether the use would be considered 'fair' under the copyright law (Lessig, 2000).

It is not clear, however, that the technologies and legal structures that make such levels of control notionally available have been all that effective. Indeed, it can be argued that they never will be. Every piece of code written can be deciphered: often with not much more expertise than that acquired in undergraduate computer studies, or by those who see doing so as a social challenge. What is required alongside technical and legal rights

management structures is a social consensus about fair Internet trading, and a market structure within which what consumers value is made available at a reasonable price. Bollick notes that:

> … practically every technical protection measure has been broken to date; [and] we should expect illegal copies of practically any content work to be readily available on the Public Internet. People will choose convenience and service over piracy if the service enables them to use content as they want to use it at a reasonable price (2001).

This view is entirely consistent with established research in the area: DRMSs that take due regard of user interests and needs, especially so as not to unduly infringe the right of freedom of thought, expression and communication, that provide high levels of accessibility and usability, and that provide end users with perceived value for cost, are likely to be the most successful (cf: for example CIRCIT, 2001).

Key Components of a DRMS

International work is proceeding apace on development of the complex sub-systems needed for implementing a comprehensive digital rights management system. What follows is an attempt to describe the main components of that work. It is necessarily summary in form, and sometimes over simplifies in the interests of accessibility. Readers who want more precise technical detail are advised to consult the detailed documentation referenced in this section.

Identifying the work (and its components)

Functionally, a digital object has to be able to be identified for

- managing intellectual content (its own, and that of which it makes use),
- linking customers with content suppliers,
- facilitating electronic commerce, and
- enabling automated copyright management for the work and its various components for all types of media.

In the physical domain, identifying a work can be a relatively simple task: its components at least "cohere" in some tangible object. In the digital environment, this is not the case.

A glance at Figure 1 below which is taken from the ONIX international standards for representing and communicating book industry product information in electronic form (EDItEUR, 2001a) shows how complex it is merely to describe a traditional, physical publication to meet these levels of functionality in a digitally accessible form:

```
<Product>
    <RecordReference>1234567890</RecordReference>
    <NotificationType>03</NotificationType>
    <ISBN>0816016356</ISBN>
    <ProductForm>BB</ProductForm>
    <DistinctiveTitle>British English, A to Zed</DistinctiveTitle>
    <Contributor>
        <ContributorRole>A01</ContributorRole>
        <PersonNameInverted>Schur, Norman W</PersonNameInverted>
        <BiographicalNote>A Harvard graduate in Latin and Italian literature, Norman
        Schur attended the University of Rome and the Sorbonne before returning to the
        United States to study law at Harvard and Columbia Law Schools. Now retired
        from legal practice, Mr Schur is a fluent speaker and writer of both British and
        American English</BiographicalNote>
```

```
    </Contributor>
    <EditionTypeCode>REV</EditionTypeCode>
    <EditionNumber>3</EditionNumber>
    <LanguageOfText>eng</LanguageOfText>
    <NumberOfPages>493</NumberOfPages>
    <BASICMainSubject>REF008000</BASICMainSubject>
    <AudienceCode>01</AudienceCode>
    <ImprintName>Facts on File Publications</ImprintName>
    <PublisherName>Facts on File Inc</PublisherName>
    <PublicationDate>1987</PublicationDate>
    <Height>9.25</Height>
    <Width>6.25</Width>
    <Thickness>1.2</Thickness>
        <MainDescription>BRITISH ENGLISH, A TO ZED is the thoroughly updated,
        revised, and expanded third edition of Norman Schur's highly acclaimed
        transatlantic dictionary for English speakers. First published as BRITISH SELF-TAUGHT
        and then as ENGLISH ENGLISH, this collection of Briticisms for
        Americans, and Americanisms for the British, is a scholarly yet witty lexicon,
        combining definitions with commentary on the most frequently used and some
        lesser known words and phrases. Highly readable, it's a snip of a book, and one
        that sorts out – through comments in American – the "Queen's English" –
        confounding as it may seem.</MainDescription>
        <ReviewQuote>Norman Schur is without doubt the outstanding authority on the
        similarities and differences between British and American English. BRITISH
        ENGLISH, A TO ZED attests not only to his expertise, but also to his undiminished
        powers to inform, amuse and entertain. – Laurence Urdang, Editor, VERBATIM,
        The Language Quarterly, Spring 1988 </ReviewQuote>
    <SupplyDetail>
        <SupplierSAN>1234567</SupplierSAN>
        <AvailabilityCode>IP</AvailabilityCode>
    <Price>
        <PriceTypeCode>01</PriceTypeCode>
        <PriceAmount>35.00</PriceAmount>
    </Price>
    </SupplyDetail>
</Product>
```

Figure 1: ONIX Product Information Guidelines, sample <Product> record from EDItEUR 2001a

An additional set of epublication codes adds to the complexity when categorizing a digital product by defining 23 common types of epublication in 7 standard formats. These codes, an essential part of the description of ebooks, "are maintained separately because of the speed of change in this area" (EDItEUR, 2001b). Beyond this new etype and format information, the very architecture of emerging technologies may introduce the need for additional information about the publication's components and their relationships to other creative works.

Granularization describes the capacity of digital technologies to deliver smaller "chunks" of more targeted information to the end user (sometimes another machine) and the likelihood that users will selectively consume smaller pieces of a work in an era where there is an information glut rather than a scarcity. Many of these uses of small pieces of information were once the domain of the "fair dealing or use" provisions of physical copyright regimes. But, online digital technologies make the dynamic **pooling and blending** of "granules" of information not only viable through automation, but also potentially commercially valuable.

An example may make this clear: I arrive in a strange city by plane, take out my mobile phone and connect to a local information service my "next generation" telephone

company provides, and for which I pay a fee. This service is, in fact, a published web page that has no content provided by the mobile phone company. It is accessed because of my phone's ability to locate me. Its only content is "mined" from other websites and includes, in this simple example,

- weather information from the local television station,
- an entertainment guide from the local newspaper,
- taxi telephone numbers from a competitor's phone directory, and
- information about local hotels who pay for the privilege of having their websites "mined" and contact information listed.

Should the providers of the weather, entertainment and taxi information benefit from the fee I pay my phone company for the service, and the advertising revenue provided by the hotels? If so, each component of their published websites needs to be able to be identified as much as the publication as a whole.

Convergence is the term used in the media industry to describe the way that, in new interactive digital media, not only content but also "fields of interest and business hitherto separated are now melting into one field of information/transaction activities …This topples down old business models and value chains" (Schmid, 2000). When we consider that an epublication can also take advantage of convergent media to incorporate digital content not found in traditional publications, such a video, sound, and hyperlinks, it is plain that the range of copyright material able to be incorporated in epublications (and hence requiring rights treatment) has expanded considerably.

Deep linking, made possible by convergence, involves providing a link to a web site that goes directly into the structure of the site, possibly even pointing directly to a media source, bypassing the site's homepage and the page structure of the site. Using such a link, it is possible (intentionally or accidentally) to avoid rights protection information and mechanisms put in place by the creators and publishers of materials. Most commercial concern about the practice, however, seems to stem from deep linking's potential to reduce advertising revenues for the linked website

Courts in various jurisdictions have taken different approaches to dealing with deep linking: StepStone, an online recruitment company, recently obtained an order in the German Courts to prevent a competitor, OFiR from "deep linking" to the StepStone website The injunction was secured on the basis of existing European Union legislation concerning copyright protection. However, just a year ago in the US, Ticketmaster was unsuccessful in legal proceedings brought against Tickets.com for "deep linking" albeit that, in that case, Ticketmaster's online terms and conditions did not preclude deep linking – a provision included in many online terms and conditions.

The worldwide web is a complex medium of communication, combining as it does elements of the types of communications channels once the particular domains of "broadcasting" and "publishing". There is a sense in which the "public broadcast" component of its very architecture (the http – hypertext transfer – protocol) makes it strange that legal remedies against deep linking are even being sought when simple technological solutions are available. If someone does not want others to deep link to their material, the soundest advice they could be given is "Don't put it on the web" or, at least, don't put it there with a static URL (uniform resource locator – the now well known

IP [Internet Protocol] address that usually begins "http://") without password or similar protection.

In line with the need to develop taxonomies that allow for these new aspects of content identification in the digital environment, the **Dublin Core Metadata Initiative** (DCMI – http://au.dublincore.org/) is an organization that grew out of a meeting in Dublin, Ohio in 1995. It works to promote the " … widespread adoption of interoperable metadata standards and [on] developing specialized metadata vocabularies for describing resources that enable more intelligent information discovery systems" (http://au.dublincore.org/about/).

It describes any digital resource in terms of fifteen "elements", each of which can have a series of "qualifiers":

Domain	Element	Examples of qualifiers
CONTENT	1. Coverage	***Spatial:*** e.g. ISO3166 (Country names)/Getty Thesaurus of Geographic Names ***Temporal:*** e.g. start="2000-01-26"
	2. Contributor	Adams, Mary; Collins, Shane; Leonard, Liam
	3. Date	Created/Valid/Available/Issued/Modified
	4. Description	Table of Contents/Abstract
	5. Creator	Collins, Shane (ed)
	6. Format	Plaintext/Richtext/html/mpeg/msword/
	7. Type	Collection/Dataset/Event/Image/Service/Software/Sound/Text/Poem/ Interactive Resource/Web Homepage
INTELLECTUAL PROPERTY	8. Publisher	Common Ground Ltd
	8. Identifier	URI – Universal Resource Identifier, e.g. ftp://ftp.is.co.za/rfc/rfc1808.txt http://www.w3c.org/ mailto:john.smith@nozone.net news:comp.infosystems.svrs.unix
	10. Relation	Is Version Of/Has Version/Is Replaced By/Replaces/Is Required By/Requires/Is Part Of/Has Part/Is Referenced By/References/Is Format Of/Has Format
	11. Rights	"Copyright Common Ground 2001 - All rights reserved." http://www.commonground.com.au/info/legal.html
INSTANTIATION	12. Language	ISO 639-2 e.g. en-uk/en-au/es/fr/de/zh/ru
	13. Source	(A reference to a resource from which the present resource is derived)
	14. Subject	Dewey Decimal Classification/Library of Congress Headings
	15. Title	The Greatest Book Ever Written

Table 1: Dublin Core Metadata Initiative elements and examples of qualifiers (assembled from material at http://au.dublincore.org/)

The main aim of the initiative is to supplement existing methods for searching and indexing Web-based metadata. The schema readily translates into "header tags" that can be added to the code used to write web pages. These tags allow search engines and archiving systems to find online content readily.

What to do with identifiers?

It is possible to use new digital technologies to encode some of this information, identifying the work, its creator and distributor and rights treatment information and warnings within the work itself by:

- **Digital watermarking (steganography)** - which uses information invisibly embedded in the data itself that can only be removed with a consequent, severe degradation in its quality. It may for example contain information about author,

contributors and publisher, its title, and importantly for access control, who bought the work, what use of it was authorized, how and where it may be accessed, and how many times. A good digital watermark can be detected in the data even after the quality of the altered data becomes quite poor.

- **Encryption -** which scrambles information in a digital object and hides within it a key, and information about the content of the item, such as the title, author, and copyright. A prospective user needs to obtain a licence that contains the key to unlock the packaged information. The licence specifies the rights that are allowed to the user.
- **Content registration** - which relies on creators and publishers registering the very content of a work with a central agency and the use of information technologies to detect similarities in the content and structure of two digital objects.

However, it is difficult to prevent improper use, such as onward copying to unauthorized users or non-subscribers with these techniques. They are weak in terms of actual control. Imprints and watermarks may discourage abuse, hidden codings and content registration might help to detect it, but neither can be easily applied to prevent it. Minimizing abuse involves both identifying the material and controlling the way that the architecture if the Internet then allows access to it.

The **Digital Object Identifier (DIO)** is such a system for identifying and then exchanging intellectual property in the digital environment. "It provides an extensible framework for managing intellectual content in any form at any level of granularity, for linking customers with content suppliers, facilitating electronic commerce, and enabling automated copyright management for all types of media" (http://www.doi.org).

It functions a bit like a bar code in the physical world. A registration agency allocates a permanent "dumb number" in the format:

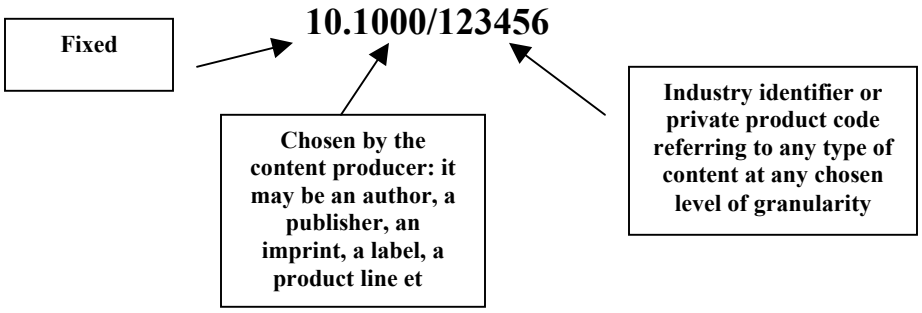

Figure 2: The structure of a Digital Object Identifier

The DOI links a unique bit of digital content with a minimum set of associated data held by the registration agency:

- An existing industry or private proprietary identification number or code
- A title, an agent and a role (e.g. author, publisher, producer)
- The type of item (e.g. a file, an abstract, an ebook, a performance)
- Its mode (text, audio, visual, audiovisual, abstract)

Changes in ownership, or treatment of the item are notified to the agency. This minimum set of metadata is public: additional metadata agreed on at an industry level, or decided individually need not be.

The DOI system uses a distributed central directory structure like that used to find web pages themselves. Every web site has a unique IP address (like 123.456.789.000) which is assigned to the server on which it sits. When you type something like "http://www.commonground.com.au/" into your web browser, the system looks up that address on an Internet connected computer called a domain name server (DNS) and finds the IP address of the machine on which the website is located. What comes after the slash (e.g. books/index.html) is the name of directory or a file on the machine with that IP address. If a web site moves to a new location all that has to be done is that the registration authority that controls domain names has to be told to "point" the address name to a new IP address.

When a digital object with a DOI changes its location or its ownership, for example, all that has to be changed is the registration information associated with it. In a similar way also to the way the architecture of the web can be used to trace "hits" on a web page, the movement of an item with a DOI around the Internet can be traced.

As an example of how the process works, the *DOI Handbook, Version 1*, (International DOI Foundation, 2001) has the DOI, **http://dx.doi.org/10.1000/182**. Here you can read in more detail about the DOI system, which in summary then, has four main components:

- Enumeration (assigning the DOI number)
- Description (supplying the minimum metadata set and incorporating the **<indecs>** scheme for rights definition)
- Resolution (looking up the address and incorporating the **Handle System** to facilitate interoperability)
- Policy (the standards, agreements and protocols necessary for the operation of registration agencies and the quality maintenance of metadata).

The International DOI Foundation (IDF) and the other major international collaboration on digital object identification, the Japan-based Content ID Forum (cIDf), agreed at a meeting in Geneva in August 2001 to collaborate on the project of building interoperable specifications for content identification and metadata that enable ecommerce and rights transactions for copyrighted information.

The DOI system works in combination with two other open protocols to deal with rights definition in the minimum data set and the complexity of transactions involving online supply chains.

Access Control

The Corporation for National Research Initiatives (CNRI's) **Handle System** (http://hdl.handle.net/4263537/4070) was chosen as the underlying resolution technology for the DOI because of its:

- "Multiple resolution capability
- Scalability
- Reliability

- Resolution speed
- Proven usage in several digital library projects
- Already [being] implemented and supported in several practical systems
- Commitment by its developers to open standards, and
- Commitment to further development." (http://dx.doi.org/10.1000/182, Section 6.4)

It is composed of a global Handle Registry run by CNRI and many local Handle services installed in much the same way a local web server is. The handles themselves used to locate digital content are in a format we already know (Naming Authority/Unique Naming Authority Identifier - e.g. "10.1000/182" where 10 is the DOI system, 1000 is the DOI code for IDF publications and 182 is the identifier for the DOI Handbook).

The Handle system also contains access control features not available in the URL system:

- read and write permission for public, authorized or no access
- time to live (TTL) and time stamp information to force reference to the source
- a <reference> capacity that can point, for example to a digital certificate or signature

Rights specification and interoperability

As already stressed, copyright is a bundle of rights. A task similar in scope to that involved for the DOI project in identifying a work is involved in specifying the rights that a creator or publisher might wish to insert in relation to a wok or components of it.

If DRMS interoperability is to be achieved, both a common understanding and a common language of rights in digital content is needed. Not only publishers, but other media creators and distributors as well want access to a variety of business models such as different fees for different reading devices, formats and renderings for a publication, superdistribution, pay-per-view, and free previews, and the DRM rights specification language (RSL) must be flexible enough to support these. It is interesting that of the sixty-six publisher requirements for DRMSs registered at the Open eBook Forum's *Requirements Portal*, fifty-five relate to the facilities of the RSL (http://www.openebook.org/requirements/viewRequest.asp).

While the Digital Object Identifier is designed to describe any form of intellectual property at any level of granularity, the **<indecs>** metadata project (interoperability of data in ecommerce systems - http://www.indecs.org) aims at generating a metadata scheme able to deal also with the even greater levels of complexity involved in rights specification across the range of transactions which confer rights or licences:

> The creator of metadata about a piece of intellectual property will want to be sure that the accuracy and effectiveness of the information he creates (often at substantial cost) can survive intact as it negotiates a range of barriers. A serious approach to the problem needs to support interoperability of at least six different types:
>
> - Across media (such as books, serials, audio, audiovisual, software, abstract works, visual material).
> - Across functions (such as cataloguing, discovery, workflow and rights management).
> - Across levels of metadata (from simple to complex).
> - Across linguistic and semantic barriers.

- Across territorial barriers
- Across technology platforms (2000).

The need for these various types of interoperability was highlighted when, last year, a French court ordered Yahoo to stop French users viewing or participating in any auctions of Nazi-related memorabilia and to screen them from "any other site or service that may be construed as an apology for Nazism". The French court's decision was made despite Yahoo's objections that the Internet servers for Yahoo's auction sites are based wholly in the United States. Unable to screen French users selectively, Yahoo now restricts sales of Nazi merchandise on its auction sites, and has gone to the US courts seeking rulings on whether the French court has authority over the content carried on US based web servers (http://www.newsbytes.com/news/01/168967.html).

In similar interventions to control content:

- Chinese citizens are encouraged to get on the Internet, but access to overseas sites is strictly controlled and what users post online is closely monitored (Kalathil & Boas, 2001);
- North Korea has decided to ban the Internet altogether: with no servers, no connections are possible, although the government does maintain a few propaganda sites on Japanese hosts.
- A few privileged Burmese users connect to the Internet through a sort of Intranet controlled by MPT, the national telecommunications carrier which is, in turn, under the direct control of the military junta. Foreigners in the country may only access email through MPT as well;
- Singapore and Saudi Arabia filter and censor Internet content;
- In Iran, the Ministry of Information's Data Communication Company of Iran screens and filters pornographic and opposition sites. Access providers are also required to prevent access to immoral or anti-Iranian material (Reporters sans Frontières [RSF], 2001);
- Australian Internet service providers (ISPs) may not provide online gambling services and must ensure content complies with censorship regulations (*Broadcasting Services Act* 1992).

A thorough discussion of content control is beyond the scope of this chapter, but one of the types of interoperability that a DRMS must have is the ability not only to specify the rights of creators and publishers and consumers, but also the ability to manage cross-jurisdictional legal and regulatory rights restrictions.

The grammar of the <indecs> system could manage rights restriction, for example, as a "situation", but it is much broader than that. It has seven "primitive entities" (described at http://www.indecs.org/pdf/schema.pdf, p.13):

ENTITY	Something which is identified
Percept	An entity which is perceived directly with at least one of the five senses
Being	An entity which has the characteristics of animate life; anything which lives and dies

Thing	An entity without the characteristics of animate life
Relation	The interaction of percepts and/or concepts; a connection between two or more entities
Event	A dynamic relation involving two or more entities; something that happens; a relation through which an attribute of an entity is changed, added or removed
Situation	A static relation involving two or more entities; something that continues to be the case; a relation in which the attributes of entities remain unchanged
Concept	An entity which cannot be perceived directly through the mode of one of the five senses; an abstract entity, a notion or idea; an abstract noun; an unobservable proposition which exists independently of time and space

Table 2: The <indecs> primitive entities framework

This framework, then, can describe the various entities and relations involved in the commercial and legal transaction that occurs when people deal with stuff:

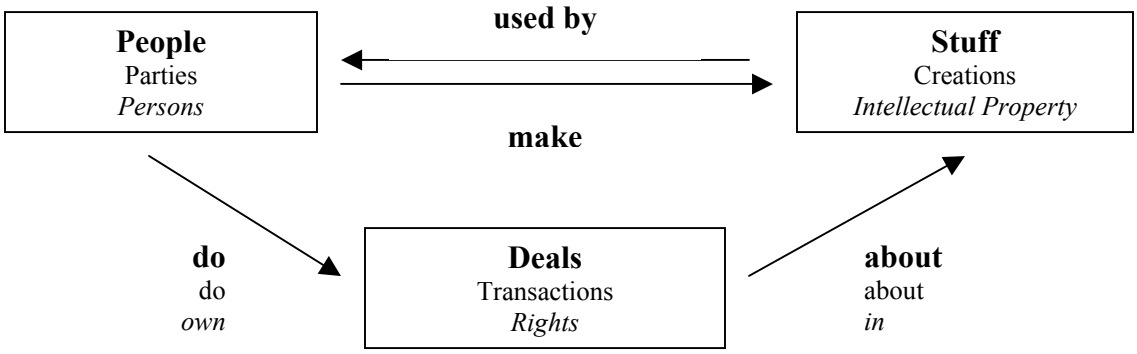

Figure 3: <indecs> commercial and legal "views" of a basic transaction

While the Digital Object Identifier is concerned with "stuff", and there are established and developing systems for identifying people, it is the capacity of <indecs> to systematically treat with "doing deals about", in a range of views that is the core strength (and focus) of its approach.

Identifying the buyer or user

Public key infrastructure (PKI) is an already growing architecture for transmitting digital content electronically by providing:

- authentication – the user knows who sent an item
- integrity – the item has not been altered in any way
- non-repudiation – the sender cannot later dispute that they sent the item
- confidentiality – only the intended recipient can open the item.

In this system of **digital certificates** and **signatures** and Certificate Authorities, a user is given two electronic "keys" that are usually asymmetric (though they can be symmetric): a public key, and a private key. The keys operate to allow the controlled two-way flow of digital information:

- **The Private Key** is used to sign items and decrypt items. It remains in the physical possession of the owner and is protected by the owner.
- **The Public Key** is kept in public key certificates and can be distributed freely and openly. It is used to verify signatures and encrypt items.

Australian standards for public key authentication frameworks are under development by Standards Australia (http://www.standards.org.au, AS 4539 series), and the Commonwealth Government has established the Gatekeeper evaluation framework for use of public key technology in Commonwealth agencies. The Gatekeeper Security Working Group has identified specific standards for:

- asymmetric key exchange;
- symmetric keys;
- key generation;
- proof of identity (POI);
- key storage; and
- protective security.

The Australian Government, for example, already accepts digital certificates from banks, and Certificates Australia (a subsidiary of Baltimore) and e-Sign Australia (a subsidiary of Verisign) have been accredited to entry-level status and a number of other companies are currently under evaluation.

DRMSs and privacy

DRMSs are designed to enhance the secure operating environment for transactions with rights protected works and other subject matter, and hence to enhance the efficiency of information markets. Generating user trust is far more complicated than simply ensuring provider protection. Indeed, if people's unwillingness to provide credit card information over the Internet (even over a secure server) is any example, it could be postulated that there is an inverse relationship between the amount of technological security built into a system, and user perceptions of the trustworthiness and security of the system.

For example, in Australia most people have both a fair measure of trust in, and a realistic assessment of the risks involved in the use of postal mail. Most people do not lock their letterboxes, but neither would they be likely to send $1000 in cash through the mail. The trust arises from confidence in the integrity and systems of the national postal authority, the legal and regulatory environment within which postal mail operates, and a fair community understanding of what risks the system can bear.

People need similar purchase on and trust in digital systems to which they are asked to supply valuable personal information if they are to be prepared to use them.

As Vora et al.(2001) have noted:

> …a number of the attempts to break the security of rights enforcement schemes were initiated because of growing public awareness of being `watched' by rights enforcement schemes. DRM systems, which currently protect only the rights of content providers, need to also protect the rights of consumers to be freer from legal liability and to be successful among consumers whose privacy awareness is growing dramatically. The very technology used to protect content provider rights can, and should, be used symmetrically to protect consumer privacy.

After a brief Indian summer, where it might have seemed, though, that technology and commerce would combine to diminish this symmetry, the protection of individual privacy has come to the fore again. The 1999 class action filed against Real Networks after the New York Times revealed that the Real Media Jukebox assigned users a globally unique identifier (GUID) when they downloaded its software. The company's privacy policy was only amended after the revelation to read:

> We may use GUIDs to understand the interests and needs of our users so that we can offer valuable personalized services such as customized RealPlayer channels. GUIDs also allow us to monitor the growth of the number of users of our products and to predict and plan for future capacity needs for customer support, update servers, and other important customer services.

The lawsuit and consumer pressure led to Real Networks offering a software patch to block transmission of the GUID (http://news.cnet.com/news/0-1006-200-1426571.html?tag=rltdnws).

In this context, and in the wake of the European Union's Directive 95/46/EC which provides that member countries will not transfer data to other jurisdictions unless similar data protection measures are in place (Article 25), recent Australian legislation has adopted internationally recognized data privacy principles. In general terms these principles provide that:

- Necessary information is only collected unobtrusively with full disclosure of purpose and use;
- Use of information is for the disclosed purpose or a reasonably expected related purpose;
- Reasonable steps are taken to ensure that information collected and used is accurate, complete and up to date;
- Reasonable security measures are in place to protect the information;
- Policies for the management of personal information are documented and open;
- An individual is able to access and correct his/her information;
- Unique identifiers are not assigned;
- Individuals must have the option of not identifying themselves when entering transactions;
- Information may only be transferred to organizations in other jurisdictions bound by similar principles; and
- "Sensitive information", information about racial or ethnic origin, political opinions, membership of a political association or professional or trade association or union, religious or philosophical beliefs or affiliations, sexual preferences or practices, for example, is only collected with informed consent.

(cf: the information privacy principles added to section 14 of the *Australian Privacy Act* 1988 and applying to government agencies (Part III, Section 14), or the *Victorian Information Privacy Act* 2000 (Schedule 1) which applies more broadly).

The Australian Privacy Commissioner is currently enquiring into how well developing PKI meets these criteria (Office of the Federal Privacy Commissioner, 2001). Key issues identified include the compliance of registration agencies who collect evidence of identity, tracking of usage through digital certificates and the possibility of them becoming unique identifiers like a national identification card, the security of agency logs and access to them for law enforcement purposes, "function creep" where social expectations disadvantage those who choose not to access PKI, consumer choice of systems and platforms and pseudonymity and anonymity.

This latter issue of whether people have the choice of remaining anonymous online has attracted some legal attention of late. Courts so far have issued mixed rulings on whether people have a right to post anonymous criticism. In July 2001, overturning a lower court's decision, a state appeals court in New Jersey ruled that Yahoo did not have to reveal the names of critics of Dendrite International who posted to its board, citing free speech protections (http://news.cnet.com/news/0-1005-200-6548390.html?tag=rltdnws). A California judge ruled in August 2001 that Yahoo does not need to reveal the identities of some message board posters who posted critical messages about Oklahoma-based legal company Pre-Paid Legal Services can remain anonymous. Pre-Paid had argued that it needed to know the identities of the posters to determine whether they had revealed company trade secrets. However, the Electronic Frontier Foundation, representing the anonymous posters, countered that they were merely criticizing the company as allowed by the First Amendment to the US Constitution, and that Pre-Paid was trying to silence its detractors by bullying them (http://news.cnet.com/news/0-1005-200-6863061.html).

Developments in user identification and authentication coupled with electronic tracking technologies may, indeed, make the collection of extremely granular, personally-identifiable digital asset usage information a simple task Whether or not doing so is a good idea or not is quite problematic. The creator or publisher who was at first attracted to the prospect by what seemed an obvious way to broaden a market might also start to consider the legal and demand vulnerabilities that it involves. DRMSs do not need to invade consumer privacy or scuttle anonymity to prevent piracy and fraud.

Rights authorization

As has already been argued, open standards in rights specification and rights authorization is likely to allow for more robust, trustworthy and functional rights clearing.

In addition, Robert Bolick (2001) has provided a cogent summary of the criteria the American Association of Publishers believes the IDRM Research Group should implement for any rights authorization technology:

- **Interoperability** - the consumer should be able to access content from different sources and in different formats without needing different hardware or software to do so

- **Security** - adherence to accepted security practices should be able to be verified by a reputable, independent third-party.
- **Key management** - support for multiple scenarios for PKI management, including: individual transactions, bulk retailing and third parties.
- **Off-line usage** - the DRM system should support asynchronous operations. A user should not have to remain continuously online to access authorized content.
- **Rights persistence** - once a consumer has acquired the right to content, the consumer should have continued access to it, regardless of changes in the status of author, publisher, retailer, hardware, or software and beyond technological adjustments.
- **Open logging** - any market participant should be able to collect, package and redistribute anonymous usage and market information to others.
- **Privacy** - consumers should control personally identifiable information collection and use. Anonymous purchase should be possible.
- **Consumer tools** - consumers will be provided with tools to manage, store, catalogue and otherwise process their ebook content and metadata.
- **Multiple business model support** – it should be possible to locate content and metadata anywhere in the network and to transmit content via current and new communications infrastructures.
- **Choice of multiple security levels** – the DRMS should provide multiple security levels, authentication, digital signatures and watermarking.

The association seems to strike a reasonable balance between wanting to protect the integrity of intellectual property and its owners and creators from commercial piracy, while advocating the rights of consumers to privacy and of the community to the free expression of ideas and the free flow of information.

A better mousetrap?

While waiting to see whether technological initiatives can deal adequately with the complexity of people, stuff, rights and transactions involved in the trade in creative works, others already dealing in online dissemination are trying less hi-tech paths through the rights authorization labyrinth.

The 'try and buy' distribution model developed in the use of **shareware** for software is a case in point. Sometimes this model involves limited protection measures, such as the distribution of a version of the software that is missing features or that cannot be used more than a certain number of times or days.

Primal Publications (http://www.primalpub.com) allow one the downloading for personal use of free short texts in Acrobat format, with the following conditions:

- You may make one (1) back-up copy of the Primer.
- You may read the Primer on as many different computers as you see fit, so long as only two copies of the Primer are in existence at any one time.

- You may not modify the Primer in any way shape or form.
- You may not redistribute the Primer without the express written consent of Primal Publishing and the author.
- If you read, print out, or otherwise keep the Primer, you are obligated to pay the shareware fee (http://www.primalpub.com/aboutprimal/legal.html, viewed 26 August 2001).

The Primal Publications notice also serves as a good example of expressing the legal obligations of the purchaser of copyright material in **plain English**. The movement to do this with legal statements has a long history, but unfortunately much of the momentum acquired in the past quarter of a century in legislative drafting and the like seems to have escaped those who design the agreements often found on web pages. There is a growing feeling among online distributors that, if an online product represents fair value for money, and if the obligations expected of the purchaser are clearly detailed, compliance is reasonably assured.

With this type of process in mind, Amazon has established an "**honour system**" to collect small payments from website visitors who agree to simple obligations such as these (http://s1.amazon.com/exec/varzea/subst/fx/home.html/104-1591015-4338352, viewed 26 August 2001). Online content publishers add a clickable button to their page that allows a charge on a registered user's credit card to be aggregated in accounts registered content producers hold with Amazon. There were some seventy sites using the system in August 2001, including significant content suppliers such as Bartleby for online literary works, BedandBreakfast.com for accommodation bookings, and Amazon's own Internet Movie Database.

Stephen King's experiment with *The Plant* may not be the best example of how an honour system could work, but it was certainly notorious enough to deserve comment. King had asked online readers to contribute US$1 for each chapter of the online novel, relying on their ethical acceptance of the principle that creators should be paid for their work. Over 75 per cent of readers had made the payment, when King doubled the price to US$2 for Chapter 4 of the book, and there was extremely hostile reaction when he decided not to proceed for the present, leaving the book incomplete and some readers US$7 out of pocket. Trust is a two-way relationship.

As the name implies, this **freeware** is distributed freely, with no usage cost. It may, however, have licensing agreements that specify how material may be used, and especially conditions that assert the copyright and protect the moral rights of creators (cf: Chapter 1).

Public domain materials are those where copyright has expired or where the copyright holder allows them to be freely copied and distributed. Unlike freeware, public domain works can be modified or repackaged for sale.

The Massachusetts Institute of Technology OpenCourseWare (MIT OCW) initiative is an example of making published materials available in the public domain with some of the characteristics usually associated with freeware. Consistent with general MIT policy, "ownership of Intellectual Property developed by faculty, students, staff, and others participating in MIT programs, including visitors, with the significant use of funds or

facilities administered by MIT will vest with MIT". However, MIT President, Charles Vest, acknowledges that they will be modified and incorporated into new courses:

> MIT OCW will provide an extraordinary resource which people around the world can adapt to their own needs. A new engineering university in Ghana, a precocious high school biology student in New Mexico, an architect in Madrid, a history professor in Chicago, or an executive in a management seminar down the hall at MIT will find MIT OCW materials freely and instantly available. It will complement and stimulate innovation in ways that cannot even be envisioned at this point, and will make it possible to quickly disseminate new knowledge and educational content in a wide range of fields (http://mit.edu/newsoffice/nr/2001/ocwfund.html, viewed 26 August 2001).

MIT course materials that are used in the teaching of almost all undergraduate and graduate subjects available on the web, will be disseminated free of charge, to any user anywhere in the world from 2002. The stated aim of the initiative, which has substantial philanthropic funding, is as follows:

> MIT OCW will radically alter technology-enhanced education at MIT, and will serve as a model for university dissemination of knowledge in the Internet age. Such a venture will continue the tradition at MIT and in American higher education of open dissemination of educational materials, philosophy, and modes of thought, and will help lead to fundamental changes in the way colleges and universities engage the web as a vehicle for education (http://web.mit.edu/ocw/ocw-facts.html, viewed 26 August 2001).

Can DRMSs keep rights in balance?

The examples in the chapter illustrate that digital rights management systems, like all other information and communication technologies are just that: technologies. Their value is not in the mere fact that they exist but in the way they help people do what they want to do, and solve the problems they want to solve.

Can DRMSs keep rights in balance? "Not on their own!" is the simple answer that emerges from our discussion. They are always at work in a broader social, legal, and commercial context, and often these other elements of their context are more significant in shaping what people actually do than the possibilities made available by the technologies themselves.

Writing recently in *The Australian*, The Economist opined "… though it is inspiring to think of it as a placeless datasphere, the Internet is part of the real world. Like all frontiers, it was wild for a while, but policemen always show up eventually" (2001). Police, in the real world, have known for a long time that a "long arm" is merely one element of their repertoire. Good intelligence, targetted intervention, community respect, a sense of proportion, and probity to mention but a few, are equally important.

References

American Association of Publishers 2000. *Digital Rights Management for Ebooks: Publisher Requirements Version 1.0*, http://www.publishers.org/home/drm.pdf, viewed 19 August 2001.

Barlow, John P 1996. *Declaration of the Independence of Cyberspace* http://www.eff.org/Publications/John_Perry_Barlow/barlow_0296.declaration, viewed 18 August 2001

Berne Convention for the Protection of Literary and Artistic Works (1886) and the *Paris Act of 1971 as amended 1979*. http://www.wipo.org/treaties/ip/berne/berne01.html viewed 8 August 2001.

Bolick, Robert 2001. *Publishers' Requirements for Digital Rights Management,* paper presented at the W3C DRM 2001 Workshop, Sophia Antipolis, France, January 2001, http://www.w3.org/2000/12/drm-ws/pp/macgrawhill-bolick.html, viewed 18 August 2001.

CIRCIT (Centre for International Research on Communication and Information Technologies) 2001. *The User Perspective on Government Electronic Service Delivery (ESD)*, Research Report No 29, by S. Singh, R. Kelso, A. Ryan, T. Laidler, J. Burke and A. Tegart, http://www.circit.rmit.edu.au/publics/soc_obs.html, viewed 20 August 2001.

Commonwealth of Australia 1968. *Copyright Act* No. 63 of 1968 incorporating amendments up to Act No. 24 of 2001, Canberra: AGPS, http://scaleplus.law.gov.au/html/pasteact/0/244/rtf/Copyright68.rtf, viewed 19 August 2001.

Commonwealth of Australia 1988. *Privacy Act* No. 119 of 1988 incorporating amendments up to Act No. 55 of 2001, Canberra: AGPS, http://scaleplus.law.gov.au/html/pasteact/0/157/pdf/Privacy88.pdf, viewed 25 August 2001.

Commonwealth of Australia 1992. *Broadcasting Services Act* No. 110 of 1992 incorporating amendments up to Act No. 92 of 2001, Canberra: AGPS, http://scaleplus.law.gov.au/html/pasteact/0/136/rtf/BSA92Vol01.rtf, viewed 26 August 2001.

EDItEUR Limited 2001a. *ONIX Product Information Guidelines Release 2.0 <Product> record*, http://www.editeur.org/onixfiles2.0/ONIXProductRecord2.0.pdf, viewed 20 August 2001.

EDItEUR Limited 2001b. *ONIX International Epublication codes Issue 1.0*, http://www.editeur.org/onixfiles2.0/ONIXEpublicationCodes.doc, viewed 20 August 2001.

European Union 1995. 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, *Official Journal L 28* , pp. 0031 – 0050, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html, viewed 25 August 2001.

Government of Victoria 2000. *Information Privacy Act,* No. 98/2000, http://www.dms.dpc.vic.gov.au/sb/2000_Act/A00814.html, viewed 25 August 2001.

Ianella, Renato 2001. *Open eBooks Digital Rights Management Standards*, paper at Open Publish 2001 Conference, Sydney, http://www.iprsystems.com/assets/openpub2001.pdf, viewed 20 August 2001.

Illich, Ivan 1973. *Tools for Conviviality*, New York: Harper & Row, http://philosophy.la.psu.edu/illich/tools/index.html, viewed 10 August 2001.

Inglis, K.S. 1983. *This is the ABC: The Australian Broadcasting Commission 1932 – 1983*, MUP: Melbourne, ISBN 0 522 84258 5.

International DOI Foundation 2001. *DOI Handbook, Version 1, February 2001*, http://dx.doi.org/10.1000/182, viewed 24 August 2001.

Kalathil, S. and Boas, T.C. 2001. *The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution*, Carnegie Endowment for International Peace, http://www.ceip.org/files/Publications/wp21.asp, viewed 26 August 2001.

Kaplan, B. 1967. *An Unhurried View of Copyright,* Columbia University Press: New York.

Laidler, Terry 2001. "Does Copyright Have a Digital Future?" *C-2-C Creator to Consumer in a Digital Age,* Common Ground: Melbourne, ISBN 1 86335 048 9.

Lessig, Lawrence 1998. *The Laws of Cyberspace* http://cyberlaw.stanford.edu/lessig/content/works/laws_cyberspace.pdf, viewed 11 August, 2001.

Lessig, Lawrence 2000. "The Limits of Copyright" *The Industry Standard* http://www.thestandard.com/article/0,1902,16071,00.html, viewed 10 August 2001.

Loren, Lydia P. 1997. "Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permission Systems," *Journal of Intellectual Property Law,* Vol. 5, No. 1 Fall 1997.

Martin Elizabeth A. 1997. Dictionary of Law, OUP: Oxford, ISBN 0 19280 066 3.

Office of the Federal Privacy Commissioner 2001. *Privacy Issues in the Use of Public Key Infrastructure for Individuals and Possible Guidelines for Handling Privacy Issues in the Use of PKI for Individuals by Commonwealth agencies*, http://www.privacy.gov.au/publications/dpki.html, viewed 25 August 2001.

Open eBook Forum 2000. *A Framework for the Epublishing Ecology: Public Comment Draft Version 0.78*, http://www.openebook.org./members/Systems/Documents/A Framework for the Epublishing Ecology.doc, viewed 19 August 2001.

Reporters sans Frontières 2001. *The Enemies of the Internet*, http://www.rsf.fr/uk/homennemis.html, viewed 26 August 2001.

Rust, Godfrey & Bide, Mark 2000. *The <indecs> Metadata Framework: Principles, model and data dictionary,* http://www.indecs.org/pdf/framework.pdf, viewed 18 August 2001.

Schmid, Beat F. et al. 2000. *Ein Glossar für die NetAcademy*, Media Communications Management Institut, Universität St. Gallen, translated at http://www.mediamanagement.org/netacademy/glossary.nsf/kw_id_all/49, viewed 19 August 2001.

Stewart, Stephen M. 1989. International Copyright and Neighbouring Rights 2nd edition, Butterworths: Sydney, ISBN 0 406 66222 3.

Still, Viveca 2001. *Legal Challenges for the Development of Digital Rights Management Systems* W3C DRM 2001 Workshop, Sophia Antipolis, France, Monday 22 January 2001, http://www.w3.org/2000/12/drm-ws/pp/unihelsinki-still.html, viewed 25 August 2001.

The Economist 2001. Running wild, until the cyber police turn up, *The Australian*, August 17, 2001, http://www.theaustralian.news.com.au/common/story_page/0,5744,2609093%255E7583, 00.html, viewed 20 August 2001.

United Nations Universal Declaration on Human Rights 1948, http://www.un.org/Overview/rights.html, viewed 16 August 2001

Vora, P., Reynolds, D., Dickinson, I., Erickson, J. and Banks, D. 2001. *Privacy and Digital Rights Management*, W3C DRM 2001 Workshop, Sophia Antipolis, France, Monday 22 January 2001, http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html, viewed 25 August 2001.

Wark, McKenzie 2001. *The Hacker Manifesto 2.0*, http://www.feelergauge.net/projects/hackermanifesto/version_2.0/, viewed 12 August 2001.

World Intellectual Property Organization (WIPO) Copyright Treaty 1996. Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, Geneva, December 2 to 20, 1996, http://www.wipo.org/treaties/ip/copyright/copyright.html, viewed 16 August 2001.

Glossary

Acronym	Meaning
CAL	Copyright Agency Limited http://www.copyright.com.au
cc	Counter-copyright
cIDf	Content ID Forum http://www.cidf.org/english/index.html
CNRI	Corporation for National Research Initiatives http://hdl.handle.net/4263537/4028
DCMI	Dublin Core Metadata Initiative http://au.dublincore.org/
DNS	Domain name server
DOI	Digital Object Identification http://www.doi.org/
DRM	Digital rights management
DRMS	Digital rights management system
GUID	Global user identification
http	Hypertext transfer protocol (the Internet protocol on which the worldwide web is based)
IANA	Internet Assigned Names Authority http://www.iana.org/
ICANN	Internet Corporation for Assigned Names and Numbers http://www.icann.org/
ICT	Information and communication technology
IDF	International DOI Foundation http://www.doi.org/
IDRM	Internet digital rights management http://www.idrm.org
indecs	Interoperability of data in ecommerce systems http://www.indecs.org/
IP	Internet Protocol
IP	Intellectual property
PC	Personal computer
PKI	Public Key Infrastructure
POI	Proof of identity

RSL	Rights specification language
URL	Uniform resource locator (a web address)
W3C	Worldwide Web Consortium http://www.w3c.org
WIPO	World Intellectual Property Organization http://www.wipo.org/