THE UNIVERSITY OF HULL

RepoMMan Project

R-D13 / R-D15

DRM Literature Review and Investigative Report

Chris Awre

September 2007

The RepoMMan Project

Project Director:	Ian Dolphin, Head of e-Strategy, University of Hull	(i.dolphin@hull.ac.uk)
Project Manager:	Richard Green	(r.green@hull.ac.uk)
Technical Lead:	Robert Sherratt	(r.sherratt@hull.ac.uk)
Repository Domain Specialist:	Chris Awre	(c.awre@hull.ac.uk)

The Repository Metadata and Management Project (RepoMMan) at the University of Hull is funded by the JISC Digital Repositories Programme. The project is being carried out by the University's e-Services Integration Group (e-SIG) within Academic Services.

Introduction

The development of digital repositories involves the management of potentially a wide range of digital content types. These types can be classified by their MIME type or by their purpose and role amongst other means of organisation. In all cases, though, there is IPR in the content generated. As with all IPR this needs to be managed. This management is often carried out by the copyright owner of the content, or their appointed representative: for example, a book publisher will often manage the IPR on a book by one of their authors. Digital repositories are a technology intended to store digital materials generated and owned by institutions and their staff and students. Institutional IPR polices may have different nuances on exactly how copyright ownership is managed, but the IPR in the content needs to be managed regardless. Digital repositories provide both a set of challenges and a potential solution to enabling this management. This is particularly the case where the content will be exposed over the Internet for sharing with others: digital materials can be copied with relative ease and there is a need to ensure as far as is possible that their IPR is not breached. There may also be additional rights that the copyright owner wishes to lay down as a condition of access and/or use. The need to manage these rights has led to the emergence of the field of Digital Rights Management (DRM).

This document considers DRM in the context of digital repositories, and specifically the deployment of an institutional digital repository at the University of Hull. It combines two deliverables from the RepoMMan project.

- A DRM literature review, which looks at a range of literature published on DRM and related topics, to identify current trends and issues that digital repositories need to consider.
- A DRM investigative report, which takes the outcomes of the literature review and applies them to the range of digital materials that it is intended can be stored within the Hull digital repository, and that members of the University have indicated are in use within their spheres of activity.

IPR is a wide field, and there have been many reviews of the legal issues involved in the context of managing digital materials (for example see Cordiner (2006), Casey (2006)). However, the main focus of this report is the examination of the technical issues involved in managing DRM within a digital repository. This takes into account the legal issues examined elsewhere and looks at the aspects a digital repository needs to consider when putting DRM into practice. It does not, though, seek to replicate work carried out elsewhere by authors better qualified to comment.

In making available digital content held within a repository to a wider audience, there is a need also to ensure that what is being delivered is being made available by a trusted source, so that those users discovering the content are clear in their own minds that it is valid content. This sense of trust can impact on whether the DRM processes put in place are themselves trusted and accepted. This report also addresses this flip side to DRM as part of an overall approach to making sure digital repositories can become valid, secure and long-term sources of quality information.

Disclaimer

Notwithstanding the references made to various documents discussing the legal aspects of DRM, IPR and copyright, etc., this report should not be considered as any form of legal advice on these areas. Formal legal advice should always be taken to ratify the intended approaches.

Digital Rights Management

It is valid to ask why we need DRM when there are laws preventing the unfair copying of content and other breaches of IPR. Whilst these laws have proved reasonably effective in preventing illegal activities in printed materials, the ease of copying and re-use that digital content provides – one of its greatest advantages – has meant these same laws haven't had the same effect in the digital environment (Coyle, 2003). The case of Napster is a case in point. Digital content requires a technical solution to the management of the rights within it.

This view may have emerged from the commercial arena, where there has been concern and effort in addressing DRM with regard to the music industry for some years. DRM in itself is regarded as of value as a means of managing access to the increasing range of digital content now available. The OSI e-Infrastructure Working Group report (2006) regarded DRM as a core function for the delivery of the distributed e-infrastructure the report envisages developing as international research collaboration grows (notwithstanding the need to manage this across international and, hence, legal boundaries).

Taking this need on board, Digital Rights Management has been defined in the following ways, amongst others:

"*… an umbrella term that refers to access control technologies used by publishers and other copyright holders to limit usage of digital media or devices*."[1]

"*Any technology used to protect the interests of owners of content and services*."[2]

"*DRM is a term that has many meanings. To some, it is the "Management of Digital Rights", to others it is the "Digital Management of Rights". Generally speaking, DRM is a system that is used to "manage rights". Depending on the context, manage rights include:*

** A system that is used to secure and distribute protected e-books or protected media files. The rights are defined during the protection step and issued as a usage license to consumers*
** A system that is used to control access to an online service. For example a web service. Applications will need to have access to a license in order to invoke the web service*
** A accounting system that can track the rights issued and the royalties that are associated/due with those rights*"[3]

A range of definitions can also be found as part of the CEN/ISSS Final Report on Digital Rights Management (2003). One of the contributors to this report, the Music Publishers' Association (MPA) emphasises that full DRM encompasses the ability to "…securely convey and enforce complex usage rights rather than simple low-level access/copy controls", although both are required.

As can be seen from this the term DRM is used flexibly to mean a range of technical approaches to the management of rights. A wide range of technologies and approaches can be placed under its umbrella depending on the purpose for which they are being applied.

Notwithstanding these definitions that look at systems, technical or otherwise, as the basis for enabling DRM, the management of the rights involved mentioned in the third definition above is in part about determining the policies and licences that lay down the rights and how these are put into practice. In 2004, the JISC commissioned a study of how DRM developments should be taken forward in the context of the UK education and research communities (Duncan et al., 2004). Based on LaMacchia (2002), this report was structured around two key principles of DRM: the management of policies under which material will be made available,

[1] Digital Rights Management, Wikipedia, http://en.wikipedia.org/wiki/Digital_rights_management (accessed 27th Sept 2007)
[2] Digital Rights Management, Microsoft Security Glossary, http://www.microsoft.com/security/glossary.mspx#d (accessed 27th Sept 2007)
[3] DRM, XrML terms, http://www.xrml.org/reference/xrml_terms.asp (accessed 27th Sept 2007)

labelled DRM Policy Creation; and ensuring that these policies are respected by the third parties accessing the digital content involved, labelled DRM Policy Projection.

A series of stages is proposed to help address the different aspects of DRM, as outlined in Figure 1. Different technologies and technical solutions are of relevance at different stages. Each stage is at a different level of maturity and institutional digital repositories need to consider the balance between the benefit of addressing each stage and the capability, technical or otherwise, of implementing it.

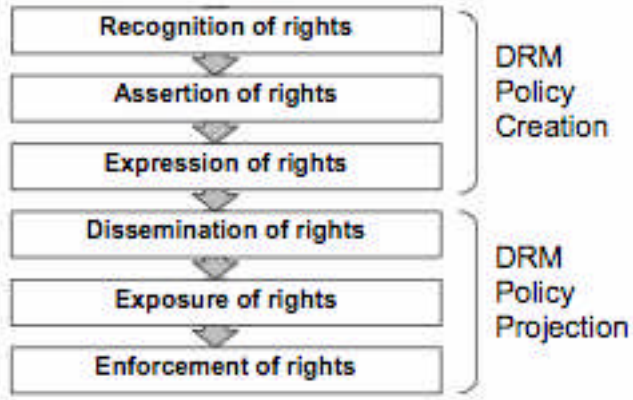

Figure 1: Stages in the DRM process

Another way of expressing this distinction, as described by LaMacchia, is through the difference between authoring expressions of rights and evaluating them, and the systems that are used to meet these two objectives. This has similarities with the approach taken by the TrustDR project in their report on The Legal Terrain affecting Digital Repositories (Proven et al., 2006), which separates out the components of DRM into rights management, rights technology, and rights projection (see Figure 2).

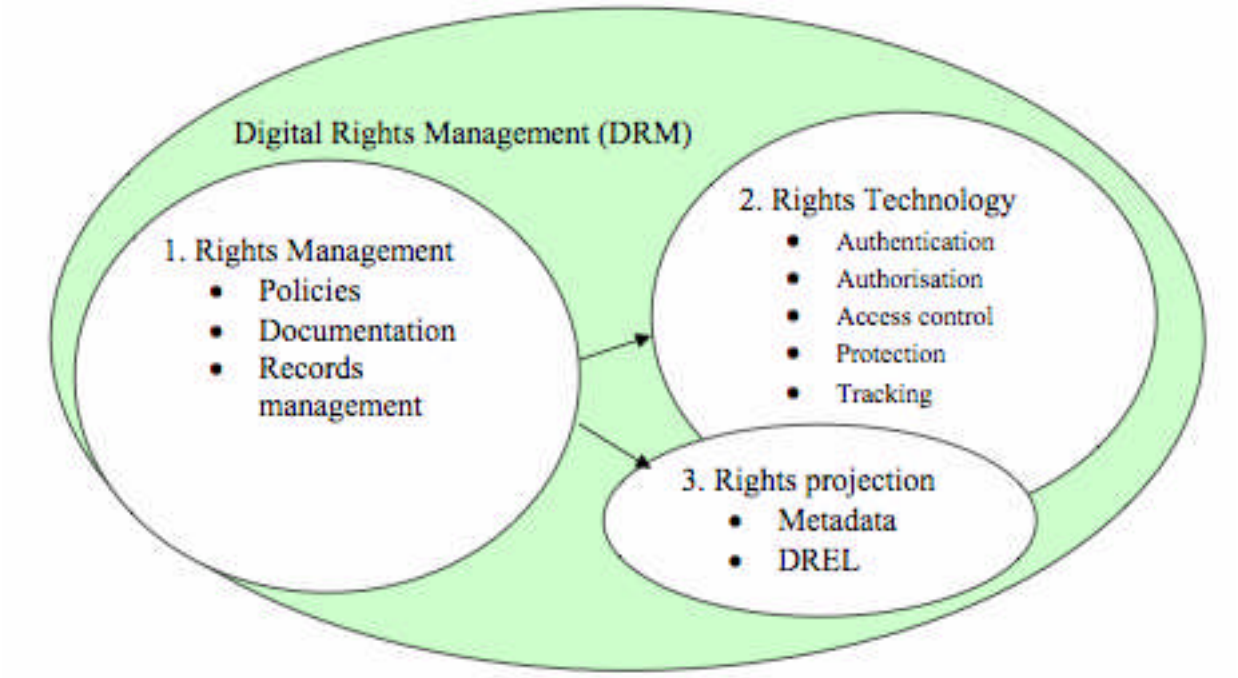

Fig.2 Elements of DRM

Whichever delineation is found to be most useful, Dripps et al. (2006), in another report from the TrustDR project, describe the differences between a functional and dysfunctional DRM framework. Characteristics of a functional framework include:

- All parties recognise IPR ownership
- Accurate recording of rights information
- Quality metadata is part of resource creation
- Culture of attribution
- Technology reflects policy and supports human activity
- A clear risk management strategy

Applying these criteria, which involve a high QA element, to the implementation of managing rights will lead to a strong base for enabling useful DRM.

Licences

In their Repositories Roadmap, Heery and Powell (2006) viewed the lack of automated DRM as being a potential barrier to the long-term take-up of repositories, which would not be able to provide the controlled access required for many institutional outputs (notwithstanding the development of open access for some). Their vision for the future of repositories encompasses the availability of machine-readable licences that repositories can act upon.

The creation and projection of policies outlined in the JISC DRM report requires the policies to be encapsulated in something that can be transmitted and understood by those viewing them. Licences fulfil this role. In a paper prepared for a JISC Legal Briefing Day, Richard McCracken (2004) talks about the primacy of the licence and licensing in managing access to digital content. This derives from the selling of digital products. Unlike when selling a book, the subscriber/purchaser does not own the digital product; they simple purchase a licence to access it. As such, the licence essentially becomes the product. The principle of assigning licences in this way applies as much to institutional digital repositories as to commercial operations. McCracken emphasises the need to be very clear about the scope of the licences developed for disseminating digital content emanating from the University so that the licences are effective and clearly understood. This scoping is best placed within the context of a Digital Policy Management framework, an approach discussed at a BL/JISC/UKOLN workshop in 2006 (Beagrie and Bide, 2006).

Various digital collections have been made available under their own licences over the years. A good example of the range is the many image collections available for educational use. The Pixus image portal project[4] in 2003 developed a demonstrator search system across six image collections. When clicking through from the thumbnail retrieved in a search to the hosting image collection the user often had to agree on the licence under which the images were made available; these differed by collection due to the different owners. When tested with teachers within an FE College as part of the FAIR Enough project[5] the feedback revealed a lack of interest in using the images concerned due to having to deal with and understand these different licences.

The complexity that has arisen in dealing with different licences has led to the need for mechanisms to help deal with this. An ongoing project, RELI[6], is building a pilot licence registry to help manage these, whilst a major part of JISC Collections and academic library activity is now negotiating and managing licences to the many digital resources now available.

Digital repositories can equally add to this collection of licences to help address the IPR needs of the institution and/or the author(s) concerned. Whilst many repositories have focused on

[4] Pixus image portal demonstrator project, 2003, http://www.jisc.ac.uk/whatwedo/programmes/programme_portals/project_image_portal.aspx (Accessed 28th Sept 2007)
[5] FAIR Enough project, 2002-4, http://www.westerncc.ac.uk/fairenough/ (Accessed 28th Sept 2007)
[6] RELI project, 2007-9, http://www.lboro.ac.uk/departments/dis/disresearch/RELI/ (Accessed 28th Sept 2007)

open access, those repositories that store learning materials and images, for example, have a need to be sure about how they wish to disseminate these materials and under what terms. The JORUM national learning object repository has developed detailed licences to manage the resources placed within it[7,8], and is also keeping its own eye on how and what DRM systems might meet their requirements (Halliday, 2006). Much of the need for this detail derives from the academics who create the materials wishing to know who is using them, plus wishing to exert a degree of control in how they are used or modified. This academic concern has occurred in discussions at the University of Hull regarding datasets as well[9]. Whilst open access does not have such a need for licensing, it is recognised that licensing and DRM are important to enable openly accessible material to be used with confidence and protect against plagiarism or improper changing of the content by others (Friend, 2004; Poynder, 2005).

The JISC DRM report and participants at two JISC workshops on rights in the digital environment (Charlesworth, 2005) both called for common licences and templates that can be used, based on wide consultation. There is a dilemma in developing a generic licence, though, in its ability to meet the needs to working with different digital content types. An increasingly popular approach is the use of the Creative Commons licences[10], which have been adapted to work with UK law[11]. These licences allow individuals and organisations to state what can be done with resources in the areas of attribution, commercial use and derivation. Thus far universities have not widely adopted Creative Commons licensing, though individuals within them have done moreso. It is interesting to note that Lawrence Lessig, one of the creators of Creative Commons, is not in favour of DRM systems because of the restrictions these can place on accessing and using digital content. Lessig contributed to a conference entitled "Content Licensing: Cultivating the Creative Commons" at Queensland University of Technology in 2005 (Fitzgerald, 2005) where he is quoted as saying, "Never in our history have fewer exercised more power over our culture than now." The conference also contained a series of papers on the role of Creative Commons within government and public institutions, which aimed to demonstrate that licensing along the lines of Creative Commons can stimulate innovation (Cunningham et al, 2005).

Recognising that the basic Creative Commons licences may not suffice for specific areas of education and research, companion initiatives have emerged to meet these needs. The Science Commons[12] and ccLearn[13] initiatives, both based at MIT, are looking to create open platforms for the exchange of digital content within scientific disciplines and for learning & teaching, respectively. It should also be recognised that Creative Commons licences are not a panacea, and careful consideration needs to be taken to ensure their appropriateness (Korn and Oppenheim, 2006).

Digital rights expression languages

Having a licence is one matter, making this available, the expression of rights as described in Figure 1, is another. Licences can be made available in paper format or electronically. Paper licences are limited to the subscribing body, most often the Library within a University. Electronic licences can make management easier and allow the licence to be closely associated with the digital content it refers to. For this to happen there needs to be a way in which the licence can be expressed electronically. Digital rights expression languages (DRELs) have been designed to address this issue.

---

[7] JORUM User Terms of Use, http://www.jorum.ac.uk/user/termsofuse/index.html (Accessed 28th Sept 2007)
[8] JORUM Contributor Terms of Use, http://www.jorum.ac.uk/contributors/ctermsofuse/index.html (Accessed 28th Sept 2007)
[9] Personal communication regarding a dataset generated as a result of research within the Department of History
[10] Creative Commons, http://creativecommons.org/ (Accessed 28th Sept 2007)
[11] Creative Commons UK, http://creativecommons.org.uk/ (Accessed 28th Sept 2007) NB, note distinction between licences applicable in England & Wales and Scotland.
[12] Science Commons, http://sciencecommons.org/ (Accessed 28th Sept 2007)
[13] ccLearn, http://learn.creativecommons.org/ (Accessed 28th Sept 2007)

Karen Coyle (2003), in a paper derived from a talk given at the Library of Congress, explains that whilst software used for opening files can be used itself to control how individual files are used, e.g., Adobe Acrobat or Microsoft Reader (often applied to e-books), the controls available are limited. A more flexible means of expressing a license is required: DRELs meet this need.

Coyle goes on to describe two of the most common DRELs now used, ODRL and XrML, whilst a JISC Techwatch study on DRELs (Barlas, 2006) also reviews existing approaches and the options available currently.

- Open Digital Rights Language (ODRL)[14] was developed by Renato Ianella in 2000 and is backed by a consortium of over 200 companies. It is a generic rights expression language based around an extensive vocabulary of terms describing the terms under which a piece of digital content can be used, with the aim of being flexible enough to encompass many different licence approaches.
- eXtensible rights Markup Language (XrML)[15] came out of work by Mark Stefik in the late 1990s. It is considered to be a meta-language, insofar as it is more abstract than ODRL and can be used as the basis for the development of DRELs for more specific purposes.

Whilst ODRL, as its name suggests, is being developed in an open way and is available to all who wish to use it, the rights to XrML is owned by the company ContentGuard. There has been debate about whether ODRL can be considered to be based on XrML because of the latter's abstract nature, and doubts remain about the relative freedom to use ODRL. XrML is widely used in commercial circles, by Microsoft and acting as the basis for the development of the MPEG 21/5 DREL[16] used within the multimedia industry. It is also the basis of an ISO initiative, ISO REL[17] because of its abstract nature. Unfortunately, no mapping between these DRELs is yet available.

For a DREL to be useful it requires a vocabulary to help it express the terms of the licence being encapsulated within it. ODRL has its own data dictionary, as these vocabularies are sometimes called, whilst ISO REL relies on the rights data dictionary developed as part of the MPEG 21 development by Rightscom in 2004[18]. This development came out of the <indecs>2rdd initiative started in 2002 (Coverpages, 2002).

All the DREL developments described above have used XML as the basis for their development. The Creative Commons licences have their own XML and other encodings (as well as plain English versions), which can be considered a specific instantiation of a DREL around these licences. An ODRL version of Creative Commons exists[19]. Other specific instantiations are being developed, for example work being carried out by the GeoDRM working group to develop a reference model[20].

DRELs set out to enable the capture of rights within an XML structure that can then be associated with the digital content the rights pertain to. In examining this in the context of open access publishing and author rights, the RoMEO project proposed its own rights metadata (Gadd et al., 2004), though eventually proposed adoption of Creative Commons due to its wide uptake. In the specific context of relations between publishers and libraries, NISO, the Digital Library Federation (DLF), EDItEUR and the Publishers Licensing Society formed a Licence Expression Working Group[21] in 2006, following a NISO workshop on Digital Rights Expression

[14] ODRL, http://www.odrl.net/ (Accessed 28th Sept 2007)
[15] XrML, http://www.xrml.org/ (Accessed 28th Sept 2007)
[16] MPEG 21/5 DREL, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm#_Toc23297977 (Accessed 28th Sept 2007)
[17] ISO REL, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36095 (Accessed 28th Sept 2007)
[18] MPEG RDD, http://www.rightscom.com/Default.aspx?tabid=1172 (Accessed 28th Sept 2007)
[19] ODRL Creative Commons profile, http://www.odrl.net/Profiles/CC/ (Accessed 28th Sept 2007)
[20] ODRL Geospatial Working Group, http://www.odrl.net/Profiles/Geospatial/ (Accessed 28th Sept 2007)
[21] NISO Licence Expression Working Group, http://www.niso.org/committees/License_Expression/LicenseEx_comm.html (Accessed 2nd Oct 2007)

in May 2005[22] that itself examined the requirements of the library and publisher communities for the expression of rights and what these should be. The aims of the Working Group are to:

- Monitor and make recommendations regarding the further development of standards relating to electronic resources and license expression, including but not limited to the ERMI and EDItEUR work.
- Actively engage in the development of the ONIX license messaging specification.

The reference to ONIX in these terms derives from the development, by EDItEUR, of the ONIX for Licensing Terms DREL[23], which itself took its lead from an earlier examination of Electronic Resource Management (ERM) requirements through the DLF's ERM Initiative (ERMI)[24]. ONIX for Licensing Terms has been the topic of extensive development in the past two years, in part through two JISC projects within the PALS Programme[25]: its first manifestation is ONIX for Publisher Licences (ONIX-PL), which provides a means for expressing publisher licences in an XML format, and for which there is now an open source tool, OPLE[26], to facilitate editing. The JISC projects helped to develop software to assist in editing the ONIX-PL file, and separately mapped a sample publisher licence (Wiley)[27] and the JISC Model Licences for e-journals, datasets and e-books into ONIX-PL[28]. Two workshops in 2006 as part of the PALS projects discussed ONIX-PL with different audiences: the Electronic Expression of Licensing Terms workshop at Loughborough University (Smith and Probets, 2006) addressed the needs and views of academic librarians, whilst a BIC workshop on Standards for the Electronic Expression of Licensing Terms addressed publisher issues[29].

Though trends and initiatives like ONIX for Licensing Terms are emerging, there is, thus far, no hard and fast agreement or consensus on which DREL is most useful for different circumstances and it is the requirements at hand that determine which will be most effective. In a white paper to the Library of Congress Coyle (2004a) lays out a framework to help guide this decision-making. Institutions and their repositories must be guided by their needs and local interest in constructively managing and enabling access to digital content.

Identifiers and watermarking

One of the issues that arose in the original NISO workshop on Digital Rights Expression was the need for unique identifiers to allow digital content to be correctly identified so that licences are correctly associated with the item. Paskin (2003), in a chapter from a report on DRM for the EU, states,

"Identifiers and metadata are prerequisites for DRM… Interoperable DRM requires a persistent means of identification and structured description."

This view builds on earlier recognitions of the link between electronic rights management and digital identifier systems (Gervais, 1999). In a white paper for Copyright Agency Limited in Australia, Dalziel (2004) describes the benefits of using DOIs to support DRM whilst warning that identifiers themselves are not the entire solution to providing DRM. He expresses a view gathered from the literature that identifiers are more useful in supporting the Management of Digital Rights (which includes the use of DRELs as well), as opposed to the Digital Management of Rights, which encompasses authentication, watermarking and encryption.

---

[22] NISO Digital Rights Expression Workshop, http://www.niso.org/news/events_workshops/RE-report.html (Accessed 2nd Oct 2007)
[23] ONIX for Licensing Terms (including details of ONIX-PL), http://www.editeur.org/onix_licensing.html (Accessed 2nd Oct 2007)
[24] DLF ERMI, http://www.diglib.org/standards/dlf-erm02.htm (Accessed 2nd Oct 2007)
[25] JISC PALS Programme, http://www.jisc.ac.uk/whatwedo/programmes/programme_pals2.aspx (Accesse 2nd Oct 2007)
[26] The ONIX-PL Editor, http://ople.sourceforge.net/ (Accessed 30th Oct 2007)
[27] Expression of Wiley Licence in ONIX-PL, http://www.editeur.org/onix_licensing_JISC.html (Accessed 2nd Oct 2007)
[28] ONIX-PL mappings of JISC licences, http://www.editeur.org//ONIX-PL_JISC/mappings.html (Accessed 2nd Oct 2007)
[29] BIC workshop presentations, http://www.bic.org.uk/events-news.html#1 (Accessed 2nd Oct 2007)

There are many authentication and authorisation systems that can facilitate DRM through managing a user's identity and the extent to which any one user can access particular digital content: indeed, such systems were considered synonymous with DRM by the OSI E-Infrastructure Working Group (2006). It is not intended to address authentication within this review in its own right due to the scale of the area concerned, though the links with DRM emerge in related discussions (see references to XACML and Shibboleth in other sections). Encryption is also not considered here for the same reasons – Coyle (2003) emphasises that encryption itself does nothing to actually prevent copying, the mainstay of DRM systems, although it clearly has its place within an overall system managing rights and controlling access. Wolf et al. (2007) propose that watermarking may have complementary benefits to DRM systems, adding persistence once an item has moved outside a controlled DRM environment or system and facilitating the tracking of digital items. The incorporation of a watermarking process into DRM is at the heart of a feasibility investigation of using Web Services for DRM systems by Kwok et al. (2004). Bing (2004) has proposed the use of 'copymarks' as an equivalent to watermarks embedding the level of protection is claimed by the rights-holder that would also have the same level of persistence.

Storing and disseminating rights

In associating electronically-expressed rights with digital content there is a need to store the XML files concerned and then to disseminate the rights alongside the content when it is passed from system to system. With the exception of technologies such as watermarking it is nigh on impossible to guarantee that the rights will remain attached once the content leaves the confines of the system carrying out the DRM. Digital repositories have been implemented in many cases as part of a commitment towards open access, although they may also provide different levels of controlled access according to need. Learning object repositories, for example, are rarely open access in the same way as repositories containing research outputs such as e-prints are.

In supporting the discovery process, repositories, like other content sources, make metadata available to support discovery and access to what they hold. Metadata records are associated with the digital content, and digitally expressed licences can be associated in the same way as a part of or as an extension to the metadata record a digital object has. Within Dublin Core there is a rights element, dc:rights, for:

"Information about rights held in and over the resource. Typically, rights information includes a statement about various property rights associated with the resource, including intellectual property rights." (DCMI, 2006). The rights element can be refined using the following terms:

accessRights	Information about who can access the resource or an indication of its security status.
licence	A legal document giving official permission to do something with the resource (recommended practice is to identify a licence using a URI)

Additional elements can be used as follows to record information about rights pertaining to the digital content in question:

dateCopyrighted	Date of a statement of copyright (this is a refinement of the date element)
provenance	A statement of any changes in ownership and custody of the resource since its creation that are significant for its authenticity, integrity and interpretation.
rightsHolder	A person or organization owning or managing rights over the resource.

As can be seen, one of the elements within Dublin Core is provenance. This is a very important aspect on disseminating rights, allowing those accessing digital content to understand where it comes from and what rights may be associated with it. This is especially

useful where rights statements are not clear or have been lost and allows tracing back to prevent inadvertent breaches of rights. The Open Archives Initiative – Protocol for Metadata Harvesting (OAI-PMH) has the ability to record the provenance of a harvested collection of metadata as part of its 'about' container[30].

```
<about>
  <provenance
     xmlns="http://www.openarchives.org/OAI/2.0/provenance"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://www.openarchives.org/OAI/2.0/provenance
     http://www.openarchives.org/OAI/2.0/provenance.xsd">
    <originDescription harvestDate="2002-02-02T14:10:02Z" altered="true">
     <baseURL>http://the.oa.org</baseURL>
     <identifier>oai:r2:klik001</identifier>
     <datestamp>2002-01-01</datestamp>
     <metadataNamespace>http://www.openarchives.org/OAI/2.0/oai_dc/</metadataNamespace>
    </originDescription>
  </provenance>
</about>
```

Collection description metadata also has the capability of providing information about where a digital resource has come from, or at least what else it is connected to, and allows the dissemination of rights about the collection. The RSLP Collection Description Schema, for example, contains an attribute, cld:accessControl, that is a sub-property of the dc:rights term mentioned above. This can record "a statement of any access restrictions placed on the collection…"[31]. It can also record provenance in terms of previous ownership through its attribute cld:custodialHistory.

Dublin Core is set up to hold relatively limited rights information in the ways shown, and link elsewhere to additional detail, such as a licence set up using a DREL. This allows clear statements of rights, but does not easily permit DRM to the extent of managing how the digital content is used. Linking to licences allows generic licences such as Creative Commons to be used without the need to store the rights information directly with the content itself. But this does not permit licences to be applied that are specific to the content.

The METSRights XML schema[32] was designed at Stanford University to accompany METS records for digital content resources (Coyle, 2004a). Its aim is to provide a way of communicating rights information between information professionals rather than to end-users. A draft was released in September 2006 and is, in part, intended to fill the gap whilst the development of DRELs is ongoing.

Neither Dublin Core nor METSRights has the intention of enabling rights statements that are machine-actionable, a requirement of full DRM systems, and a task that DRELs such as ODRL and XrML look to achieve to some degree. A markup language similar to these DRELs, XACML (eXtensible Access Control Markup Language), can also be used to express access control policies based on pre-defined rules. Although not intended as a means of encoding licences, XACML can be used within DRM systems to manage who can gain access to content and, in principle, put licences into practice. Digital identity systems for managing user identity have started to consider XACML and companion languages such as SAML and SPML as part of systems controlling access to systems in general (Windley, 2005).

The Fedora digital repository system has an XACML engine as part of its architecture to facilitate access control within the repository, though the complexity/flexibility of XACML means the best way of applying it is still in development: there is active engagement with this

[30] OAI-PMH about container, http://www.openarchives.org/OAI/openarchivesprotocol.html#Record (Accessed 19th Oct 2007)
[31] RSLP Collection Description Schema, http://www.ukoln.ac.uk/metadata/rslp/schema/ (Accessed 19th Oct 2007)
[32] METSRights, http://www.loc.gov/standards/mets/news080503.html (Accessed 2nd Oct 2007)

issue within the Australian RAMP project[33]. Fedora also has the ability to store separate metadata records alongside the associated digital object as part of its digital object model (Fedora Development Team, 2005). Hence, licence metadata records can be linked to digital objects as required.

Although able to manage rights within a repository, XACML cannot be used to pass rights information to others outside the repository through the discovery process. DRELs can be used for this, though they are reliant on the dissemination protocols being used correctly maintaining the link between the licence metadata and the content metadata. Where rights are simply stated within a metadata record using Dublin Core these are one and the same; where a separate DREL is used there needs to be a clear understanding of what should be delivered when a user is searching the repository.

Common search protocols such as Z39.50 will retrieve relevant Dublin Core fields as agreed between the Z-server and Z-client. Common profiles such as Bib-1 include a number of Dublin Core fields, and dc:rights is given a use attribute of 1111[34]. The system searching using Z39.50 would need to know how to deal with this field, though, in order for the rights information to be correctly presented.

This need to ensure rights are presented in the correct context informed work within the RoMEO project[35], with specific reference to the use of OAI-PMH for the dissemination of metadata from open access repositories. An earlier white paper to the Technical Committee of the OAI by Bird (2001) had proposed the hosting of a small set of licences to support standardised adoption of these amongst data and service providers. There was concern, though, about incorporating rights within the protocol itself for fear of alienating individual groups. The RoMEO project proposed its own method for incorporating Creative Commons licences within OAI-PMH (RoMEO Rights Solution, 2003), a piece of work that led to the release of a further white paper on OAI-rights (Lagoze et al., 2003) and the development of appropriate guidance in 2005 (Lagoze et al., 2005). Note that this guidance relates to rights in the metadata itself, not the digital content the metadata describes. Rights pertaining to the content need to be disseminated in conjunction with the content itself if and when this is accessed or transferred between systems.

Assigning rights so they can be stored and disseminated is a matter for local implementation. As with all metadata, the default position over time for digital repositories has been to present metadata fields to the content owner and ask them to enter appropriate information. The RepoMMan project has sought to capture as much metadata as it can automatically and present this to the content owner for editing, thereby stimulating interaction (Green, 2007). Although not a part of the original project, it is reasonable to apply the same principle to rights information: pre-set licences could be presented for the content owner to select from.

The Sakai Collaboration and Learning Environment[36] aims to enable just this. When a user creates a resource within the system they are asked to supply metadata as described above. One of the options, as demonstrated in Figure 3, is to select the terms on which the resource can be used from a drop-down menu. This can guide usage within Sakai, and how a resource is used outside the system as well if downloaded.

[33] RAMP authentication and authorisation modules for Fedora, http://www.ramp.org.au/ramp-s-authentication-and-authorization-modules-for-fedora (Accessed 4th Oct 2007)
[34] Bib-1 attribute set, http://www.loc.gov/z3950/agency/defns/bib1.html (Accessed 2nd Oct 2007)
[35] RoMEO project, http://www.lboro.ac.uk/departments/ls/disresearch/romeo/ (Accessed 2nd Oct 2007)
[36] Sakai, http://www.sakaiproject.org (Accessed 4th Oct 2007)

Figure 3. Assigning copyright to resources

Personal and institutional collections

The RepoMMan project envisages a personal repository space where users can manage their own works prior to 'publishing' them to the public repository under open or controlled access. Survey findings within the project (Green, 2006a), and validated within similar work by the CD-LOR project (Margaryan, 2006), highlight the potential benefit of a repository offering this restricted area in a repository for personal protection, with the user then choosing when to open it up to others. Beagrie (2005) describes the increase in personal digital collections and the need to enable better management of these, to support preservation as much as regular use. As he quotes, this development is a realisation of the foresight expressed by Vannevar Bush (1945) in his description of the 'memex' as an addition to a person's memory. Issues of rights in the content arise, especially where there is overlap between personal, work and externally related content, and in relation to where the collections are maintained – who owns the systems the collections are maintained on?

The boundary between personal and institutional collections is more emphasised when submission of the digital content concerned is effectively the same process as transferring it from a personal store to an institutional one. There is a concomitant loss of control that needs to be addressed. The JISC-funded Rights and Rewards in Blended Institutional Projects project[37] at Loughborough University investigated the issues faced by academics depositing within an institutional repository. Alongside developing their own rights solution to ease concerns about depositing learning materials in a repository, they carried out a survey of perceived copyright ownership to identify whether academics felt they or the institution owned copyright in the materials in the first place (Loddington et al, 2006). They quote Monotti and Ricketson (2003) and state that,

"…as a general rule IPR rests with "the creator of the material in question – the invention, book, design etc, as the case may be, unless there is some employment relationship subsisting between the creator and another party, in which the ownership vest in the employer". Therefore, inherently, the University owns the copyright of teaching materials because it is created during the course of employment. This is of course unless the Institution has an alternative policy stating that teaching materials are jointly owned by the academics and the institution or solely by the academics."

Only 26% of those surveyed realised this, with the majority indicating their uncertainty (54.9%): interviews at the University of Hull for RepoMMan also suggested uncertainty in this area (Green, 2006b). The University of Hull IPR Policy states (University of Hull, 2006):

"Unless there are specific agreements to the contrary, the university owns

- all intellectual property generated by staff during the course of their employment
- all intellectual property generated by registered students during the course of their study
- all intellectual property generated by staff and students other than in the course of employment or study if substantial university resources have been used"

[37] Rights and Rewards in Blended Institutional Repositories project, http://rightsandrewards.lboro.ac.uk/ (Accessed 19th Oct 2007)

However, it also states:

"The sharing of information is an important part of the university's work. The university is committed to freedom of publication provided that any IP arising is suitably protected."

This and other such policies have not generally been designed or tested in face of using digital repositories to any great extent and it will be necessary to engage the relevant authorities further to better understand what is and what is not reasonable.

If Universities do own the digital content produced through employment, then the management of personal collections is significantly altered. And yet there are now a myriad of tools available that encourage the building of personal digital collections (e.g., Zotero[38] and related bibliographic management software packages), albeit that most of these focus on citations and references rather than actual digital content. The Scholar's Box[39] is an example of software where citations can be mixed with 'real' content, iTunes one that focuses entirely on content that the individual holds. In the latter, there are clear delineations about who owns the material and what you can do with it. Could the same model apply within universities, so making it clearer how personal digital collections should be managed? OCLC have recognised this issue and are running their Personal Research Collections Program[40] during 2007. The outcomes from this will be of great interest. Dealing with personal collections within a digital repository as a whole has also been addressed within the Paradigm project (Thomas and Martin, 2006).

DRM systems and architecture

The careful working through of the DRM stages described above, however they are delineated, will be needed to ensure that DRM does what it is designed to do to meet everyone's needs. Existing commercial DRM systems have been used inappropriately at times to limit access to digital content, partly in response to paranoia about illegal copying (MacColl, 2001). DRM systems have a position in law that can override copyright law and fair dealing, an aspect that is currently protected under EU law (British Academy, 2006). Fair use, copying for personal use, can be completely prevented by locked down DRM systems, though there have been proposals for ways in which such systems can take on board the additional contextual information that is required to enable them to be more flexible (e.g., Tyrväinen, 2005). The clash between DRM and copyright law is also described by Ganley (2002), who emphasises that much discussion around DRM systems tends to be about systems that are to come rather than those actually being used. Thus, the flexibility that DRM systems could provide commercially is not yet realised and frustration has ensued whilst content is locked down in the interim. Part of the problem is the proprietary nature of the majority of DRM systems in use, which limits their use and requires users to interact with multiple systems through multiple vendors of digital content (in the commercial context). Ganley goes on to discuss and propose alterations to DRM systems that can avoid invasions of privacy that come about from collecting information about the user. The privacy issue is raised alongside concerns about security and limitations on choice in INDICARE's Consumer Guide to DRM (INDICARE, 2006) as matters for individuals to be aware of when purchasing and/or accessing digital content.

The lack of standardisation in DRM systems has been widespread. Common use of DRELs, such as the use of XrML by Microsoft for its widely e-Book reader[41] will assist, although the ongoing patent issues regarding XrML (Coverpages, 2006) will not make the landscape simple. There is no shortage of standardisation efforts: a CEN/ISSS report on DRM listed 28 initiatives encompassing various commercial, standards, technical and disability organisations (CEN/ISSS, 2003). Stamp (2003) reviews the state of the DRM market at that time, and

[38] Zotero, http://www.zotero.org/ (Accessed 19th Oct 2007)
[39] Scholar's Box, http://www.raymondyee.net/wiki/ScholarsBox (Accessed 19th Oct 2007)
[40] OCLC Personal Research Collections Program, http://www.oclc.org/programs/ourwork/newmodes/personalcoll/default.htm (Accessed 19th Oct 2007)
[41] Microsoft, XrML and e-books, http://www.microsoft.com/reader/developers/info/das.mspx (Accessed 4th Oct 2007)

concludes that even though there are many options, all of them are susceptible to being hacked. If one instance of the software is hacked the system loses its usefulness wherever it is implemented: uniqueness in software is considered the only way to address this.

The use of DRM systems to restrict access except on the terms of the rightsholders has had an impact on education in two ways (Fisher and McGeveran, 2006): firstly, concern about piracy has led to a reluctance to grant educational users access to works for study and research except on full economic terms; and secondly has had the knock-on effect of educators themselves looking to use DRM systems and strict licensing to restrict access to content they generate or disseminate. The relatively restrictive architecture of course management software is regarded as being a contributing factor here. This dynamic appears to contradict the perceived need for the DRM industry to address the concerns of end-users in their use of information on a fair basis (Foroughi et al., 2002). The issues of DRM systems and their effect are ongoing. Arkenhout et al. (2004) have proposed scenarios to help guide policy development within the European Union, covering potential eventualities from a weak DRM to a strong DRM environment on the creation and distribution of information. They propose potential actions as well, including making hacking a DRM system legal if it can be shown that copyright law is being breached through the practice of DRM, a reverse of the current position as described at the start of this section.

There has been much consideration given to DRM architectures in discussions around the implementation of DRM generally, largely with the aim of enabling standards-based distributed DRM systems. The creator of ODRL, Renato Ianlella, proposed a functional architecture (Ianella, 2001) that encompassed a framework modelled in three areas (see Figure 4), each of which can be broken down further. Jantz and Giarlo (2005) have discussed the architecture for a trusted digital repository to enable digital preservation. Erickson (2003) reviews DRM architectures and the scope they have for permitting fair use whilst still providing the protection rights holders desire, which he finds to be eminently feasible if system developers are responsible enough to allow for it. This paper is in a special issue of Communications of the ACM[42] that addresses in some detail the relationship between DRM systems and the law, and the battle to enable fair use.

In the context of education and research, Martin et al. (2002b) have proposed a federated solution to enabling this approach by splitting responsibility of managing the rights between an origin site, where the user sits, and the resource provider, adopting the mechanisms of the Shibboleth federated access management architecture. In a separate discussion paper Martin and colleagues also look at general requirements for DRM (Martin et al., 2002a). Collier and Robson (2004) identify requirements for DRM solutions appropriate for education and research, devising a requirements matrix that can act as a checklist when considering local needs for a repository and other institutional systems (including the use of unique identifiers as discussed earlier). Looking beyond current usage, Dobratz and Neuroth (2004) highlight the need for DRM systems to be disabled in order to permit effective long-term digital preservation of content. The development of the conceptual framework for the US National Digital Information Infrastructure Preservation Program (NDIIP) also listed DRM as one of six critical technical issues that needed to be addressed (Friedlander, 2002) to enable effective preservation.

[42] Communications of the ACM, 2003, 46 (4), special issue on Digital Rights Management

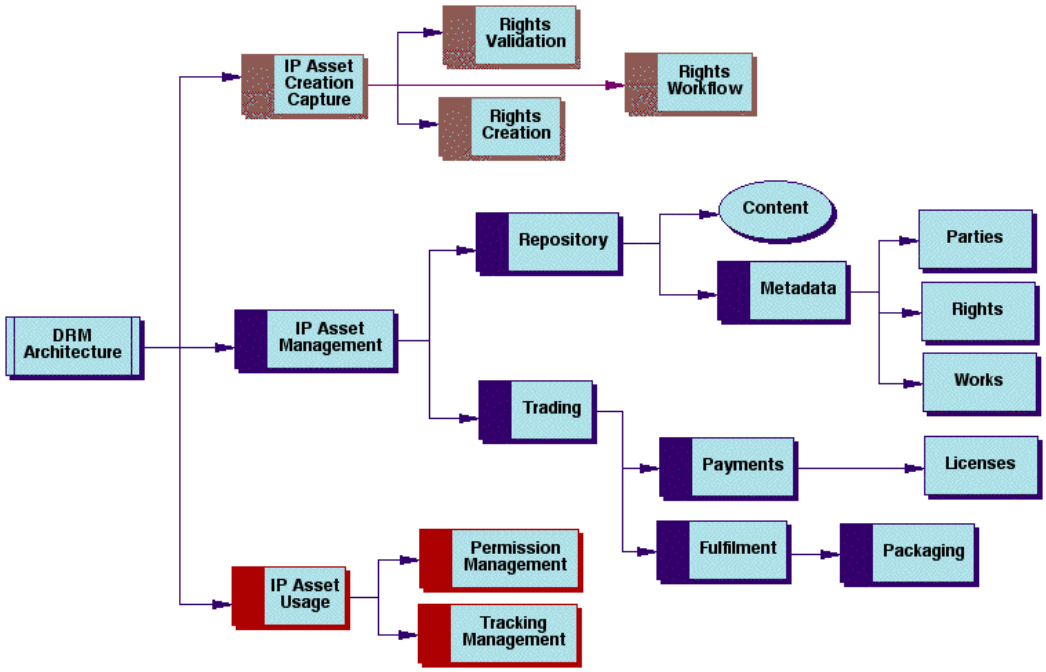

Figure 4. DRM Functional Architecture

Libraries have had a mixed relationship with DRM systems over time. Professor Pauline Samuelson raised concern at the ability of publishers to bypass libraries using DRM and control delivery of digital content directly to users (MacColl, 2001). This view does not appear to have emerged as yet, though its potential is still there. In the meantime, DRM systems can be of benefit in managing lending within a library. Coyle (2005) reports on the ability of commercial DRM systems to be used to manage the lending of e-books, where systems are used to effectively mimic a temporary sale of the e-book to the borrower with a 'return' date. The user can return it virtually after (s)he has finished with it even if this is before the end of the 'loan' period. The same principles could be applied to the lending of music or films, though this has not yet been seen in practice. DRM could also be applied to content that a library and/or its associated institutions produces and maintains – libraries are becoming publishers that need to manage access to their own digital content (Davis and Lafferty, 2002). This view is not a new one, and was addressed a decade ago as a means of addressing inherent copyright difficulties (Ramsden, 1997).

Trusted sources

In a paper in 2001, Erickson proposed a set of guiding principles for the development of DRM systems for use on the Web, in order to ensure their interoperability. These are as follows:

- The system should look to increase trust
- It should use standard formats
- It should enable human and machine readable versions of the policies to be enforced
- There should be notification of the policies to users prior to content use
- There should be openness in implementation
- The system should be complementary to current laws
- It should be transport independent
- It should enable privacy

The first of these principles can be considered a two-way process, with the DRM system enabling rightsholders to have trust in the dissemination of the content, whilst also enabling end-users to trust that the content they are receiving is correct. Notwithstanding the relative ability of DRM systems themselves to enable this latter sense of trust, digital repositories can

seek to build this trust through their policies and structures so that end-users can be confident of what they are receiving when interacting with the repository.

In his book on Digital Identity (2005), Phil Windley explores trust in the context of exchanging identity information, highlighting that trust is an inherent part of relationships between organisations and the systems they present. He proposes some properties of trust:

- Trust is transitive only in very special circumstances: you may trust someone who your friend trusts, but only on specific matters you have confidence about
- Trust cannot be shared: having trust in two people doesn't mean they will trust each other
- Trust is not symmetric: just because you trust me doesn't mean that I trust you, or vice versa
- Trustworthiness cannot be self-declared: like beauty, it is in the eye of the beholder

You can replace the people in these properties with systems and the same principles apply. The ability to capture these properties in DRELs and other machine-readable ways is, as described in this review, developing but not that mature as yet. In the context of digital identity, Windley advocates the use of governance as a means of addressing these current shortcomings, which can equally apply to DRM.

Trusted systems are being developed to serve the trust needs of both content and rights holders and end-users. Coyle (2004b) highlights some of the requirements for such systems:

- Only a trusted device (hardware and/or software) will be able to render (display or play) the digital content for the consumer
- The trusted device must only allow those actions that are explicitly granted by the rights licence
- The rights licence is issued to an identified individual

The role of such systems, as suggested by Erickson, is to improve trust on both sides of a relationship and overcome the inherent lack of symmetry in trust. Trusted DRM systems, which may be part of an operating system[43] or third party intermediary[44], seek to support the rights of content owners through ensuring the content will be used only as intended, whilst the end-user can trust the system to deliver what it says it will, even if that may be limited access compared with what is desired.

This sense of trust will often rely on more than just a DRM system controlling appropriate access. The integrity of the content being delivered can also be crucial in ensuring it is both used and attributed correctly. This has been a factor in the development of archived information for some years, where it is critical to ensure that the content archived is exactly the same as the original, and that both publishers and libraries trust the archive to carry out the necessary preservation tasks to ensure this[45]. Ross and McHugh (2005) recognise that a range of trust-related issues surrounds digital repositories:

- Security
- Authenticity
- Integrity
- Accessibility
- Documentation
- Metadata
- Disaster recovery

[43] For example, Microsoft Windows Rights Management Services, http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/rmenterprise.mspx (Accessed 10th Oct 2007)
[44] For example, Apple's FairPlay system, http://en.wikipedia.org/wiki/FairPlay (Accessed 10th Oct 2007) - though note that Apple CEO Steve Jobs has called on the music industry to remove their requirement for DRM.
[45] For example, see http://www.diglib.org/preserve/criteria.htm (Accessed 10th Oct 2007)

They observe that all of these can benefit from clear and continuous risk management to address these issues and any others that might arise over time.

In this context of developing effective digital preservation and curation systems the Research Libraries Group (RLG) and National Archives and Records Administration (NARA) in the US developed their Audit Checklist for the Certification of Trusted Digital Repositories (RLG/NARA, 2005, revised Center for Research Libraries, 2007), which has attracted wide attention. The co-chair of the Task Force that developed this, Bruce Ambacher, has reviewed its development and associated unresolved issues, advocating that government archives should take a lead in carrying out the audit to demonstrate the applicability and viability of the checklist (Ambacher, 2007). A study by the Center for Research Libraries is looking to develop the processes and activities required to carry out an audit based on this checklist (Dale, 2005). Moore and Smith (2007) are developing the PLEDGE[46] system that can carry out automated validation of the checklist using a rule-based data management system to assist its uptake. In Germany there is an equivalent effort, the nestor initiative[47], which has developed a catalogue of criteria for trusted digital repositories (Dobratz et al., 2007). This work has been linked closely to the DINI certification process (DINI, 2006). Certification is recognised as valuable, if not always easily attainable, and this issue divided the RLG/NARA Task Force. Certification, though, does require evidence, and it is clear that evidence is at the heart of enabling trust. Work undertaken by the Digital Curation Centre, complementary to the CRL work mentioned above, is carrying out pilot audits to gather further evidence on what makes a trusted digital repository (Ross and McHugh, 2006). In carrying out this work, the Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) toolkit[48] was developed, and is available for all repository managers wishing to establish their repository as a trusted source.

Summary

The ability to create, manage and disseminate digital content across the Internet has introduced a new paradigm in the management of intellectual assets and the rights held in these. This has led to the emergence of Digital Rights Management. It is important to be clear about whether it is the management of digital rights or the digital management of rights that is being addressed when referring to this term: this literature review has skimmed the surface of each, with an emphasis on the former. Adopting the existing paradigm of financial protection found in copyright law generally, DRM systems have tended to favour a lock-down approach when the digital medium offers a more flexible approach. As quoted in 1997,

"With the development of trusted system technology and usage rights languages with which to encode the rights associated with copyrighted material, authors and publishers can have more, not less, control over their work." (Stefik, 1997)

The debate continues over whether this control restricts access to those users that authors and publishers have control over or knowledge of, or whether it encourages authors to share more openly with colleagues wherever they may be by extending their sense of trust, an approach favoured by the open access community and advocates of licensing such as Creative Commons. The related issue of trusted authority in a source of digital content may influence this. Lynch, in a paper in 2001, stated.

"The integration of trust and provenance into information retrieval systems is clearly going to be necessary and, I believe, inevitable. If done properly this will inform and empower users; if done incorrectly, it threatens to be a tremendously powerful engine of censorship and control over information access."

By demonstrating the value gained by using open trusted repositories and similar systems it may encourage authors to place trust in such systems for managing and disseminating their

[46] PLEDGE project, http://pledge.mit.edu/ (Accessed 10th Oct 2007)
[47] nestor, http://www.langzeitarchivierung.de/index.php?newlang=eng (Accessed 10th Oct 2007)
[48] DRAMBORA toolkit, http://www.repositoryaudit.eu/ (Accessed 10th Oct 2007)

own work, and remove the fears that often drive more stringent DRM solutions. Appropriate and simple adoption of licensing to build trust is key to enabling this.

The University of Hull Digital Repository and DRM

Introduction

In developing the University of Hull digital repository it is important and necessary that issues of DRM and licensing are addressed. Digital repositories offer storage and access enhancements over currently employed systems. The increased access that a repository offers through exposure on the Internet beyond the boundaries of the host institution requires that there is a full understanding of the impact such exposure can have: an understanding of IPR issues and how to address these will give confidence in how a digital repository can be used and exploited to its full extent for the benefit of the institution.

The literature review conducted as part of the RepoMMan project has revealed much useful information. It is clear that the field of DRM, and general IPR, remains unclear in regard of institutional digital repositories, though there appear to be clear pointers toward establishing best practice in the context of the law as it currently stands. This section of this document comprises deliverable R-D15, the investigative report on the use of DRM, and reviews the development of the University of Hull digital repository in the context of the findings from the literature review. This leads to a suggested set of best practices to help inform our own repository's development and others where applicable.

DRM and the University of Hull Digital Repository

It is clear from the literature that Digital Rights Management can cover a wide variety of practices and systems. Taking a lead from the definition of DRM provided on the XrML website it is useful to consider the position of a repository under both interpretations of DRM.

1. Management of Digital Rights

In making digital content available over the Internet, digital repositories expose content in way that allows its re-use: access to the content does not just imply a view onto it, but the ability to make a copy that can then be stored and made accessible through different systems. It is important that content owners are clear about the limits they wish to impose on how this access is permitted and what actions they will permit. It is the purpose of licences to lay out what is and what is not permitted: it is the role of DRELs to express these terms in a way that can be disseminated with the digital content and understood by those taking the copy of the content.

In the context of open access there may be few limitations placed upon the content; this, after all, is the aim of open access. However, as Friend and Poynder showed in their articles, making something available on open access does not remove the responsibility of ownership or the need to be clear about what can be done with the open access article in question. Can it be copied, can it be changed, can it be re-used for commercial purposes, etc.? Whilst many repositories have exposed articles via open access without any obvious detriment, a large proportion of those articles have no protection under licence from anyone who chooses to make use of such articles in a way not intended. Applying a licence to digital content exposed through a repository makes it clear what is being made available and how the content can be used once exposed.

Creative Commons licences have been developed for this purpose, albeit that their remit is broader than materials held in digital repositories. In the context of an institutional digital repository, it is uncertain whether or not licences such as Creative Commons, which were designed for use by individuals, can be effectively applied at an institutional level. Amended versions or similar types of licence may be required according to the wishes of the institution at hand. Whichever approach is taken, it is important to balance the benefits of exposure through the repository with the reasonable aims of the institution in protecting materials over which it claims IPR.

The extent to which institutions can put effort into creating their own licences and presentation of these via the use of a DREL will vary. Further work on analysing the licences used and how repositories express them will be of value to the community, especially where such licences could be shared. It is unreasonable for smaller institutions to adopt ODRL or similar in designing heir own licences, but it is reasonable for them to pick up available licences from elsewhere that can be adapted for local needs.

It is important in enabling the association of licences with digital content that the repository systems employed can enable this association and also permit the continued association once the content is exposed for access. The OAI Rights approach can enable rights on exposed metadata to be transmitted, but exposure of the licence pertaining to the content itself is harder: a click-through agreement or some type of embedding may be appropriate here alongside a clear indication through the repository interface. The Fedora repository system has the capability of storing licence metadata alongside the content, though will require adoption of clear policies on how this licence is presented to ensure attention is raised.

Another key part of the Fedora repository system, and valuable in any assignment of licences, is the application of clear, persistent, unique identifiers to the content, its associated metadata, and any associated licence(s). This allows any of these three to be clearly identified and associated once the content etc has been copied from the repository after exposure. This is particularly valuable where content is moved between repositories, a general advantage of applying persistent identifiers.

The use of licences does not, as mentioned by more than one author in the literature review, enforce adherence to the terms of the licence, but it does offer legal protection in case a breach of the licence is uncovered (and where action is taken). It is this desire to enforce that has led to the development of DRM systems, particularly by commercial content owners concerned at mis-use of their intellectual property. This is where the management of digital rights moves into the digital management of rights.

2. Digital Management of Rights

Notwithstanding the rights held in a piece of content, digital or otherwise, DRM systems seek to enforce conformance to those rights, or use appropriate technologies to prevent their breach. As highlighted in the DRM architecture by Ianella, the two key components of such enforcement are permissions management and tracking management. Permissions management can be put into practice through the use of appropriate authentication and authorisation controls to limit who can access the digital repository in the first place. Such controls increase the level of trust that a repository can have in who is accessing the content it holds and licences can take this into account. Repositories designed for open access such as EPrints have not focused on this area in great depth, as that was not their intended role. Learning material repositories, as evidenced by the Jorum, have addressed this area in greater detail as the sharing of learning materials often has greater restrictions. The flexibility of both approaches is required when dealing with multiple types of digital content, though how much flexibility is required will depend on the intended purpose of the repository: multiple repositories with different approaches to DRM may be an appropriate solution in some circumstances.

Tracking management continues to be difficult and its efficacy is reliant on the ability of the repository to embed either licence information or a tracking device, e.g., a watermark, within the content itself. This is not a simple solution and would currently require systems in addition to the repository to enable this in practice. For example, the First World War Poetry Digital Archive project[49] is making use of commercial watermarking technology from Digimarc to watermark images to guard against mis-use. Encryption is another means of tracking where there needs to be a trusted exchange of keys to decrypt the encrypted content. As Coyle pointed out in her 2003 paper encryption doesn't prevent copying, but it does add a layer of protection from mis-use.

[49] First World War Poetry Digital Archive, http://www.oucs.ox.ac.uk/ww1lit (Accessed 22nd Oct 2007)

The level to which digital management of rights is pursued will depend on the level of protection required by the institution and required for particular types of content. Different approaches will be warranted where there are many different types of digital content. It is, thus, appropriate to consider some of these in turn to identify the most appropriate path of action for each. This also addresses the issues raised within the RepoMMan project's user requirements analysis reported elsewhere.

DRM and digital content types

A. E-prints / journal articles

As the articles in the INDICARE Monitor make clear, there is value in understanding the benefits of DRM in regard of open access e-prints, so that potential mis-use of the openly accessible copies is addressed before it happens. Having said that, the aim of open access is to make e-prints openly and freely available. The level of DRM required, therefore, is likely to be at the level of a licence, the terms of which will need to be agreed by the institution for use in their repository. There may need to be more than one licence where there are disciplinary differences to take account of, or there may be a desire to expose text articles more openly than, for example, associated images

B. E-theses

There are a number of IPR issues relating to e-theses that need to be addressed before an institution should consider exposing these through a repository. There is IPR in the thesis itself, and the extent to which the student and institution itself make claim, which will depend on the terms of the institutional IPR policy. There is also an issue of how to deal with third party copyright used within the thesis. This is fine for examination, but not for publication via the Internet, where it needs to be cleared beforehand, an issue that is one of good practice by student and supervisor rather than requiring a DRM solution.

Theo Andrew (2004) produced a valuable guide to dealing with IPR in e-theses. This work has been continued by the EThOS and EThOSnet projects through the development of the EThOS Toolkit[50]. This guidance is a valuable starting point in addressing the DRM requirements of e-theses within a digital repository. As with e-prints, it is likely that a licence approach may well suffice, though this may depend on the content of the theses.

C. Exam papers

It is not always the intention that content held within a repository is intended for an external audience. In the case of exam papers the audience is an internal one, to allow current students to view what has been examined in the past. This means that a level of DRM needs to be put into place. A combined approach of appropriate authentication and authorisation coupled with terms and conditions for usage of the exam papers once downloaded would make it clear to students what limitations are in place whilst providing this valuable resource. There will need to be a particular restriction on not changing the files once copied for personal use.

D. Audio and video files

Audio and video files may, and are, emerging from various walks of university life. They can be generated for learning & teaching, by both staff and students, they can come out of research, and they may be used for marketing purposes. The approach taken to DRM for such files is thus dependent on the specific purpose of the files, and the extent to which the files can be shared with others, both within and outside the institution. To take the three use cases here as exemplars:

[50] EThOS Toolkit, http://ethostoolkit.rgu.ac.uk (Accessed 22nd Oct 2007)

- Learning & teaching – audio and video files for L&T may be limited for use within the institution, or they may be deemed worthy of sharing with others, both within the institution and beyond this. The level to which DRM is required will depend on the wishes of the institution and, in some cases, the wishes of the department or even academic involved. If intended for internal use only, then a similar approach to exam papers can be used. Where exam papers should not be changed, there needs to clear guidance in the licence associated with the content on whether alterations can be made for subsequent teaching purposes or not. These terms also need to be stated very clearly if L&T audio and video materials are to be shared outside the institution, for example via the Jorum repository. The latter has strict licence terms of its own that an institution needs to agree to to participate.
- Research – audio and video files generated from research can be treated in the same way as e-prints with which they can be associated where relevant. Again, though, the terms under which changes can be made or not need to be very clearly stated in the licence associated with them.
- Marketing – audio and video files generated for marketing purposes are, by their nature, intended for external use. This does not mean that they are available for others to make use of, though, and association of the materials with a licence stating the rights held in the digital content will make it clear under what terms materials can be re-used and/or re-purposed.

E. Datasets

Datasets can be produced as a result of a variety of activities, but most likely in the context of research activity. There has been much interest in the possibility of exposing datasets alongside the e-prints that has been investigated through other projects within the JISC Digital Repositories Programme. There are accompanying licence issues when doing so, to ensure the rights of the dataset are maintained and that it is not mis-used in any way. It is also important to maintain the connection between the dataset and the e-print(s) referring to it through the use of appropriate identifiers that can also help link the licence to both.

Datasets can also be shared in their own right without the need to associate them with an e-print, and the licence associated with it will then need to be independent of any other licences or publications. The Research Information Network carried out a investigation into the stewardship of digital research data[51] in 2007 that it is hoped will lead to a set of guidelines and principles that will make such sharing clearer and simpler to implement.

F. Committee papers

Committee papers are intended as an internal collection of digital content that is for preservation and limited access only. As such, DRM is not required per se, other than high quality an authentication and authorisation system that ensures that unauthorised individuals cannot access the papers concerned.

G. Administrative documents

Similarly to committee papers, other administrative documents are only intended for limited internal audience. Depending on the documents concerned, the authentication and authorisation system will need to be fine-grained. Aside from this means of control, the terms and conditions the institution lays down for the management of administrative documents will apply to this type of digital content, as it will for committee papers.

H. Images

Images have many of the same aspects as audio and video files described above. They can be used for and generated by learning & teaching, research and administrative purposes such as

[51] RIN consultation on the stewardship of digital research data: principles and guidelines, http://www.rin.ac.uk/data-principles (Accessed 22nd Oct 2007)

marketing. Similar approaches to managing images under these areas of use will also apply. In addition, where protection against mis-use is required, watermarking may be considered as an extra DRM precaution.

Risk analysis

The previous consideration of how DRM systems and approaches might be applied to different types of digital content emerging from a University reveals two important factors.

- That there is little need for strong DRM in the same way it has been applied in the commercial sector. Where there is a need to protect IPR in University outputs from research in exploiting it there may be a need to consider more extensive DRM systems. However, the cost of implementing such systems can be prohibitive and would need to be balanced against the perceived value of the IPR to be exploited. This is likely to be better enabled through partnership with an external DRM company rather than the University implementing its own solution.
- That there is little hard and fast guidance about how to address the DRM issues relating to other materials. Like much legal advice, the exact details need to be agreed internally by the organisation holding the IPR. There is little widespread practice that has been made public to date. This may be due to a lack of tests of the licences concerned in a court of law where there has been a breach, or it may be because institutions are still establishing their own licence arrangements and are not yet in a position to make such licences public or share them within the community.

In both cases there is an element of risk management involved in assessing the level of DRM required to effective and efficiently provide the level of protection required for any particular digital content type. The arrival of the DRAMBORA toolkit to facilitate a risk assessment of repositories can assist in addressing the relative risks of storing and making accessible digital content on a case-by-case basis.

Users and assignment of DRM

In managing a digital repository that requires DRM measures to be implemented, there is an issue of who decides what measures to implement, and how they do this. Assignment will depend on the position held on ownership of the IPR within the institution. It may be appropriate for repository managers to assign the relevant rights to a digital object prior to it being made public. However, to engage the creators of the content and to share the workload involved in doing this, a system that allows users to assign IPR statements in the same way as in Sakai (see Figure 3) will be valuable to help facilitate understanding of the need to assign rights. This approach also offers flexibility according to the various different licences agreed upon for use within the repository and applicable to the content types it holds.

Proposed DRM best practice for repository management

The approach recommended for use by a digital repository is outlined throughout this second half of this report. This is summarised below for reference, with the addition of a very important first step.

- Open up dialogue between repository management and institutional legal advisers
- Carry out a risk analysis for each area of content to be stored within the repository to assess the level of DRM required when making that content accessible, either internally, externally, or both.
- Agree on the level of DRM to be enacted for each area of content
- Develop or adapt appropriate licences for use with the content types involved. Where appropriate and where effort is available, develop both human and machine-readable versions of these
- Embed the assignment of licences within repository workflow

- Agree on and enact appropriate click-throughs and other DRM measures to be put in place for specific materials requiring them
- Monitor DRM measures at regular intervals to test their appropriateness and applicability over time

References

Ambacher, B (2007). Government archives and the digital repository audit checklist. *Journal of Digital Information*, 8 (2), available at http://journals.tdl.org/jodi/issue/view/34

Andrew, T (2004). *Intellectual property and electronic theses*. A JISC Legal report, available at http://www.jisclegal.ac.uk/publicationspage.htm

Arkenbout, E, Van Dijk, F and Van Wijck, P (2004). Copyright in the information society: scenarios and strategies. *European Journal of Law and Economics*, 17: 237-249

Barlas, C (2006). *Digital Rights Expression Languages (DRELs).* JISC TechWatch study TSW0603, available at http://www.jisc.ac.uk/whatwedo/services/services_techwatch/techwatch/techwatch_ic_reports2005_published.aspx

Beagrie, N (2005). Plenty of room at the bottom? Personal digital libraries and collections. *D-Lib Magazine*, June, 11 (6), available at http://www.dlib.org/dlib/june05/beagrie/06beagrie.html

Beagrie, N and Bide, M (2006). Digital policy management workshop. *Ariadne,* April, Issue 47, available at http://www.ariadne.ac.uk/issue47/dpm-rpt/

Bing, J (2004). Copymarks: a suggestion for simple management of copyrighted materials. *International Review of Law, Computers & Technology*, 18 (3): 347-374

Bird, S. (2001). *White paper on machine-readable rights information*, available at http://www.ldc.upenn.edu/sb/oai/rights.html

British Academy (2006). *Copyright and research in the humanities and social sciences*. A British Academy Review, available at http://www.britac.ac.uk/reports/copyright/

Bush, V (1945). As we may think. *The Atlantic Monthly*, July issue

Casey, J (2006). *Intellectual property rights (IPR) in networked e-learning: a beginners guide for content developers*. A JISC Legal report, available at http://www.jisclegal.ac.uk/publicationspage.htm

CEN/ISSS DRM Group (2003). *Digital rights management final report*. A CEN/ISSS report, available at http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/drm_fg.asp

Center for Research Libraries (2007). *Trustworthy repositories audit & certification (TRAC): criteria and checklist*. A revised and expanded version of the RLG/NARA Audit Checklist for the Certification of Trusted Digital Repositories, available at http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91

Charlesworth, A (2005). *Rights in digital environments*. A report on two workshops run by the JISC, 3 and 22 March 2005, available at http://www.jisc.ac.uk/uploaded_documents/JISC%20Rights%20in%20Digital%20Environment%20Report.doc

Collier, G and Robson, R (2004). *Digital rights management for research and education*. A MELCOE White Paper, available at https://mams.melcoe.mq.edu.au/zope/mams/kb/all/DRM%20for%20Research%20and%20HE.pdf/view

Cordiner, M (2006). *Intellectual property rights in institutional and cross-institutional multimedia repositories*. A report for WP7 of the MIDESS project, available at http://www.leeds.ac.uk/library/midess/documents.html

Cover Pages (2002). *<indecs>2rdd consortium – rights data dictionary*. A Cover Pages Technology Report, available at http://xml.coverpages.org/indecs2rdd.html

Cover Pages (2006). *Extensible rights markup language (XrML).* A Cover Pages Technology Report, available at http://xml.coverpages.org/xrml.html

Coyle, K (2003). *The technology of rights: digital rights management*. A paper based on a talk originally given at the Library of Congress, November 2003, available at http://www.kcoyle.net/topiclist.html#copyright

Coyle, K (2004a). *Rights expression languages*. A report for the Library of Congress, available at http://www.kcoyle.net/topiclist.html#copyright

Coyle, K (2004b). Rights management and digital library requirements. *Ariadne*, July, Issue 40, available at http://www.ariadne.ac.uk/issue40/coyle/

Coyle, K (2005). The role of digital rights management in library lending. *INDICARE Monitor,* 2 (2), available at http://www.indicare.org/tiki-read_article.php?articleId=95

Cunningham, S, Cutler, T, Fitzgerald, A, Hoope, N and Cochrane, T (2007). Why governments and public institutions need to understand open content licensing. In: *Open content licensing: cultivating the Creative Commons*. Fitzgerald, B (ed.), Sydney University Press, Sydney, ISBN: 978-1-920898-51-9, available at http://eprints.qut.edu.au/archive/00006677/

Dale, RL (2005). Making certification real: developing methodology for evaluating repository trustworthiness. *RLG DigNews*, 9 (5), available at http://digitalarchive.oclc.org/da/ViewObject.jsp?objid=0000068925&reqid=65586#article2

Dalziel, J (2004). *DOI in a DRM environment.* A white paper for Copyright Agency Limited (CAL) from the DOI EPICS project, available at http://www.doi.copyright.com.au/

Davis, DM and Lafferty, T (2002). Digital rights management: implications for libraries. *The Bottom Line: Managing Library Finances*, 15 (1): 18-23

DCMI (2006). *DCMI metadata terms*, available at http://www.dublincore.org/documents/dcmi-terms/

DINI (2006). *DINI certificate document and publication services 2007*. English version of original German DINI certification guide, available at http://www.dini.de/wiss-publizieren/

Dobratz, S and Neuroth, H (2004). nestor: Network of Expertise in long-term STOrage of digital resources – a digital preservation initiative for Germany. *D-Lib Magazine*, April, 10 (4), available at http://www.dlib.org/dlib/april04/dobratz/04dobratz.html

Dobratz, S, Schoger, A and Strathmann, S (2007). The nestor catalogue of criteria for trusted digital repository evaluation and certification. *Journal of Digital Information*, 8 (2), available at http://journals.tdl.org/jodi/issue/view/34

Dripps, D, Casey, J and Proven, J (2006). *Functional and dysfunctional DRM frameworks for teaching and learning materials*. A TrustDR project report, available at http://trustdr.ulster.ac.uk/work_in_progress.php

Duncan, C, Barker, E, Douglas, P, Morrey, M and Waelde, C (2004). *Digital rights management: final report*. A JISC study, available at http://www.intrallect.com/index.php/intrallect/knowledge_base/general_articles/jisc_drm_study_2004__1/

Erickson, JS (2001). Information objects and rights management: a mediation-based approach to DRM interoperability. *D-Lib Magazine*, April, 7 (4), available at http://www.dlib.org/dlib/april01/erickson/04erickson.html

Erickson, JS (2003). Fair use, DRM, and trusted computing. *Communications of the ACM*, 46 (4): 34-39

Fedora Development Team (2005). *Fedora open source repository software: a white paper*, available at http://www.fedora-commons.org/developers/

Fisher, WW and McGeveran, W (2006). *The digital learning challenge: obstacles to educational uses of copyrighted materials in the digital age*. A Foundational White Paper from the Berkman Center for Internet & Society, Research publication 2006-09, available at http://cyber.law.harvard.edu/publications/

Fitzgerald, B (ed.) (2007). *Open content licensing: cultivating the Creative Commons*. Sydney University Press, Sydney, ISBN: 978-1-920898-51-9, available at http://eprints.qut.edu.au/archive/00006677/

Foroughi, A, Marvin, A and Sharlett, G (2002). Issues and opportunities in digital rights management. Paper presented at *IS2002, Informing Science + IT Education Conference*, Cork, Ireland, June 2002, available at http://www.informingscience.org/proceedings/IS2002Proceedings/toc.htm

Friedlander, A (2002). The National Digital Information Infrastructure Preservation Program: expectations, realities, choices and progress to date. *D-Lib Magazine*, April, 8 (4), available at http://www.dlib.org/dlib/april02/friedlander/04friedlander.html

Friend, F (2004). Who protects the un-protected? Open access publication needs DRM! *INDICARE Monitor*, 1 (5), available at http://www.indicare.org/tiki-read_article.php?articleId=49

Gadd, E, Oppenheim, C, Probets, S (2004). RoMEO studies 6: rights metadata for open archiving. *Program: electronic library and information systems*, 38 (1):

Ganley, P (2002). Access to the individual: digital rights management systems and the intersection of informational and decisional privacy interests. *International Journal of Law & Information Technology*, 10 (3): 241-293

Gervais, DJ (1999). Electronic rights management and digital identifier systems. The *Journal of Electronic Publishing*, 4 (3), available at http://www.press.umich.edu/jep/04-03/gervais.html

Green, R (2006a). *R-D3 Report on research user requirements survey*. A RepoMMan project deliverable, available at http://www.hull.ac.uk/esig/repomman/documents/index.html

Green, R (2006b). *R-D4 Report on research user requirements interviews*. A RepoMMan project deliverable, available at http://www.hull.ac.uk/esig/repomman/documents/index.html

Green, R and Awre, C (2007). *D-D13 Report on feasibility of automatic extraction of object metadata*. A RepoMMan project deliverable, available at http://www.hull.ac.uk/esig/repomman/documents/index.html

Halliday, L (2006). *Digital rights management for Jorum: an update, 2006*. A Jorum project document, available at http://www.jorum.ac.uk/publications/index.html

Heery, R and Powell, A (2006). *Digital repositories roadmap: looking forward*. A report for the JISC Digital Repositories Programme, available at http://www.ukoln.ac.uk/repositories/publications/

Ianella, R (2001). Digital rights management (DRM) architectures. *D-Lib Magazine*, June, 7 (6), available at http://www.dlib.org/dlib/june01/iannella/06iannella.html

INDICARE (2006). *Consumer's guide to digital rights management: any side effects?* A publication of the INDICARE project, available at http://www.indicare.org/tiki-page.php?pageName=Downloads

Jantz, R and Giarlo, MJ (2005). Digital preservation: architecture and technology for trusted digital repositories. *D-Lib Magazine*, June, 11 (5), available at http://www.dlib.org/dlib/june05/jantz/06jantz.html

Korn, N and Oppenheim, C (2006). Creative Commons licences in higher and further education: do we care? *Ariadne*, October, Issue 49, available at http://www.ariadne.ac.uk/issue49/korn-oppenheim/

Kwok, SH, Lui, SM, Cheung, SC and Tam, KY (2004). Digital rights management in web services. *Electronic Markets*, 13 (2) 133-141

Lagoze, C, Van de Sompel, H, Nelson, M, and Warner, S (2003). *OAI-rights white paper*. A white paper of the Open Archives Initiative, available at http://www.openarchives.org/documents/OAIRightsWhitePaper.html

Lagoze, C, Van de Sompel, H, Nelson, M, and Warner, S (2005). *Conveying rights expressions about metadata in the OAI-PMH framework*. A component of the Implementation Guidelines for the OAI-PMH, available at http://www.openarchives.org/OAI/2.0/guidelines-rights.htm

LaMacchia, B (2002). Key challenges in DRM: an industry perspective. *ACM Workshop on Digital Rights Management*, available at http://www.farcaster.com/papers/drm2002/

Loddington, S, Gadd, L, Oppenheim, C., Bates, M and Manuel, S (2006). *Copyright ownership of teaching materials.* A report from the Rights and Rewards in Blended Institutional Repositories project, available from http://rightsandrewards.lboro.ac.uk/index.php?section=21

Lynch, C (2001). When documents deceive: trust and provenance as new factors for information retrieval in a tangled web. *Journal of the American Society for Information Science and Technology*, 52 (1): 12-17

MacColl, J (2001). ACM/IEEE Joint Conference on Digital Libraries, Roanoke, Virginia, Jine 24-28 2001. *Ariadne*, October, Issue 29, available at http://www.ariadne.ac.uk/issue29/maccoll/

McCracken, R (2004). *Copyright, performance rights, moral rights and your digital materials*. A paper for a JISC Legal Information Service Briefing Day, held 15th September 2004, available at http://www.jisclegal.ac.uk/publicationspage.htm

Margaryan, A (2006). *CD-LOR deliverable 7: report on personal resource management strategies*. A report for the CD-LOR project, available at http://www.academy.gcal.ac.uk/cd-lor/deli.html

Martin, M, Agnew, G, Kuhlman, DL, McNair, JH, Rhodes, WA, and Tipton, R (2002a). Federated digital rights management: a proposed DRM solution for research and education. *D-Lib Magazine*, July/August, 8 (7/8), available at http://dlib.org/dlib/july02/martin/07martin.html

Martin, M, Agnew, G, Boyle, J, McNair, J, Page, M and Rhodes, W (2002b). *DRM requirements for research and education*. A discussion paper presented at an NSF Middleware Initiative and Digital Rights Management Workshop, held September 2002, available at http://xml.coverpages.org/RE-DRMRequirements.pdf

Monotti, AL and Ricketson, S (2003). *Universities and intellectual property: ownership and exploitation*. Oxford University Press, New York, ISBN: 978-0-19826-5-948

Moore, RW and Smith, M (2007). Automated validation of trusted digital repository assessment criteria. *Journal of Digital Information*, 8 (2), available at http://journals.tdl.org/jodi/issue/view/34

OSI e-Infrastructure Working Group (2006). *AAA, middleware and DRM report*, available at http://www.nesc.ac.uk/documents/OSI/index.html

Paskin, N (2003). Components of DRM systems: identification and metadata. In: Digital rights management: technological, economic, legal and political aspects in the European Union, Becker, E, Buhse, W, Günnewig, D and Rump, N (eds.), *Lecture Notes in Computer Science*, 2770, Springer, ISBN: 978-3-540-40465-1

Poynder, R (2005). The role of digital rights management in open access. *INDICARE Monitor,* 2 (2), available at http://www.indicare.org/tiki-read_article.php?articleId=93

Proven, J, Casey, J and Dripps, D (2006). *The legal terrain affecting digital repositories*. A TrustDR project report, available at http://trustdr.ulster.ac.uk/work_in_progress.php

Ramsden, A (1997). Copyright management technologies: the key to unlocking digital works? *Ariadne*, July, Issue 10, available at http://www.ariadne.ac.uk/issue10/copyright/

RoMEO Project (2003). *Rights metadata and metadata protection solutions*. A RoMEO project deliverable, available at http://www.lboro.ac.uk/departments/ls/disresearch/romeo/

Ross, S and McHugh, R (2005). Audit and certification of digital repositories: creating a mandate for the Digital Curation Centre (DCC). *RLG DigiNews*, 9 (5), available at http://digitalarchive.oclc.org/da/ViewObject.jsp?objid=0000068925&reqid=65586#article2

Ross, S and McHugh, R (2006). The role of evidence in establishing trust in repositories. *D-Lib Magazine*, July/August, 12 (7/8), available at http://www.dlib.org/dlib/july06/ross/07ross.html

Smith, P and Probets, S (2006). *Report on the workshop 'Electronic Expression of Licensing Terms' held at Loughborough University on 22 May 2006*, available at http://www.niso.org/committees/License_Expression/LicenseEx_comm.html

Stamp, M (2003). Digital rights management: the technology behind the hype. *Journal of Electronic Commerce Research*, 4 (3): 102-112

Stefik, M (1997). Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing. *Berkeley Technology Law Journal*, 12 (1): 137 160

Thomas, S and Martin, J (2006). Using the papers of contemporary British politicians as a testbed for the preservation of digital personal archives. *Journal of the Society of Archivists,* 27 (1): 29-56

Tyrväinen, P (2005). Concepts and a design for fair use and privacy in DRM. *D-Lib Magazine*, February, 11 (2), available at http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html

University of Hull (2006). *Policy on Intellectual Property Rights*. A Human Resources Directorate policy

Windley, P (2005). *Digital identity*. O'Reilly Media, Inc., ISBN: 978-0-596008-7-89

Wolf, P (2007). Complementing DRM with digital watermarking: mark, search and retrieve. *Online Information Review*, 31 (1): 10-21