Rights metadata
Standards at last?

by Mark Bide, senior consultant, Rightscom

The term ‘Digital Rights Management’ – and perhaps even more so, the acronym DRM – is becoming an increasing liability. It is associated with applications which – in the public mind at least – act as an impediment to access to intellectual property.

I have long argued that the most important ‘rights’ that we should be seeking to manage in the network are those which characterise civil society – and above all our personal and collective rights to privacy and to be protected from fraud and other crime. For a more detailed discussion of this issue see Bide M (2004) “Digital Rights Management: preventing or enabling access?” Serials 17:2.

In the absence of a trustworthy – and trusted – infrastructure, the future potential benefits of the global network will be increasingly curtailed. I am already beginning to meet people who are regular and experienced internet users but are now saying that they never connect their laptops to the internet because they are too concerned about the security risks. The manager of a major data centre told me that they experience 30 to 50 million IP attacks on their firewall in every 24 hour period. Over 50% of the email they receive is spam.

Unless this destruction of value can be controlled – through the development of a trusted network computing infrastructure – many of the potential benefits of the network will never be realised. In this context, ‘digital rights management’ can be seen as a crucial enabling technology, not an impediment, extending much further than the protection of intellectual property into all aspects of digital policy management on the network. But what do I mean by ‘digital rights management’?

I begin by assuming that all digital content is not available to everyone to access and use in any way that they choose – regardless of whether that content is private, confidential, commercially sensitive or protected by intellectual property laws. This is certainly the case today and I believe it will continue to be the case.

This being so, we can either ‘lock up’ the content behind physical barriers which simply makes it inaccessible. Or we can create a technical infrastructure which facilitates access in accordance with policies which we have established. Even in the context of the management of content on the network, I suggest that DRM has at least four different components, a much broader definition than the one we are used to.

- A ‘policy metadata’ layer, which allows for the structured description of policies – what permissions relate to this item of content, under what conditions of use (for example, attribution, period or frequency of use, payment) and what is not permitted (for example, adaptation)
- An ‘authentication, authorisation and access’ layer – which allows for the structured identification and authorisation of different users (or classes of users) and the matching of their privileges with the permissions relating to content
- An ‘enforcement’ layer, which is the technology most commonly associated with the acronym DRM – the technology which allows policies relating to content to be enforced even after content has been released from a controlled local network into the (uncontrolled) global network
- An ‘audit’ layer, which allows activities to be recorded and compliance with policies to be monitored

The coming requirement for policy metadata was already recognised a decade ago. As long ago as 1997, a joint NISO/EDItEUR working party was established in the UK under the chairmanship of Sally Morris (now the Chief Executive of ALPSP) to explore requirements. This is the primary topic that I want to discuss in this article.

Why return to such an apparently old (and, in view of the use of the ‘m’ word, probably
intensely boring) subject at this time in imi? Because we are beginning to see straws in the wind that the time of comprehensive rights metadata is finally moving out of the theoretical into the practical realm. And one place where this is happening is in academic libraries (where DRM has long been seen as unnecessary and undesirable by librarians and publishers alike).

‘Access and use policies’ are a traditional element in the management of every library. There are many reasons why every item in a library collection may not be accessible to every library user and the uses to which different items may be put are frequently not uniform across the complete collection.

In the world of physical products, the management of these policies is relatively easily managed by physical constraints and occasional human intervention. However, libraries are increasingly finding that, to take full advantage of the opportunities that the network creates for wider access to their collections, relying on physical constraints and human intervention creates insurmountable barriers to efficient management. Physical constraints no longer provide the optimum mechanism for managing policy. Rather, they seek a technical solution to a technical problem.

The management of a physical library collection is a complex task. However, librarians have centuries of relevant experience codified in library practice, systems and tools. The management of a digital library collection is at least as complex a task but the experience – and the management tools – do not yet exist.

Among the members of the Association of Research Libraries in the United States, fully 25% of acquisition budgets is now being spent on e-resources (up from less than 4% in 1992/3). Library users are increasingly unwilling to contemplate the use of physical resources which cannot be accessed from their desk top: “if it isn't available in digital form, it doesn’t exist”!

Along with all this digital content has come a whole raft of licences from publishers, all with their own terms and conditions, individually drafted and individually negotiated. But conventional library systems have no coherent way of accommodating any of the information contained in licences and presenting it either to library users (who may well want to know what they can or can’t do with a particular resource) or to library staff (who answer to the same question but also need access to additional management information about the same resources).

In response to the challenges that this represented, many of the larger US academic libraries had started to develop their own mini-licence management systems. They then recognised that it would be much more sensible to come together to devise a common set of specifications which could be followed by the library systems vendors. And so ERMI (the Electronic Resource Management Initiative) was launched by the Digital Library Federation.

ERMI goals, set in 2002, were as follows.

- Describe architectures needed to manage large collections of licensed e-resources
- Establish lists of elements and definitions
- Write and publish XML Schemas/DTDs
- Promote best practices and standards for data interchange

The first two of these goals were substantially established in their final report published in August 2004. The major library systems suppliers gratefully seized on this report and have been building extensions to their systems which are ‘ERMI compliant’ (although the precise meaning of this term remains slightly unclear).

The intention is to make licence information actionable.

- Informing end users what they can and cannot do with resources
- Controlling access to specific resources
- Prompting staff for action where appropriate (renewal reminders, for example)

A number of very complex issues have been recognised and modelled – for example, that licences relate to electronic resources in complex, many-to-many relationships; that there is often a need to interpret ‘silence’ in licenses (where does silence imply a permission and where a prohibition); the difficulty of managing the realities of complex user groups and institutional locations.
However, a fundamental problem was not tackled entirely satisfactorily – how are licence databases best to be populated?

EDItEUR (again in collaboration with NISO) held a seminar in London in December, 2004 to explore the possibility of bringing together the work undertaken by ERMi with the ONIX for Serials family of messaging standards. My company, Rightscom, was subsequently commissioned by EDItEUR (with funding support from the Publishers Licensing Society and the JISC) to undertake a proof of concept project, to explore the possibility of developing an ‘ONIX for Licences’ message that could be used by publishers and online hosts to communicate licence terms to libraries and subscription agents.

At a workshop in London, involving librarians (including ERMi representatives Nathan Robertson of John Hopkins University and Ivy Anderson of Harvard University), publishers, subscription agents and systems vendors, explored a message structure which was the child of three ‘parents’: ONIX, ERMi and the <indecs> project.

This prototype message is based on the concepts of

- permissions  
  things that may happen  
  “you can copy this”

- prohibitions  
  things that must not happen, often exceptions to permissions  
  “you can copy this – but not for commercial purposes”

- requirements  
  things that must happen in order for the permissions to be exercised  
  “you can copy this – but not for commercial purposes – but you must report the fact that you have done so”

The generic and highly granular structure of the proposed message makes it applicable in many different contexts. It is specialised for particular applications by the specific terminology which is used in the message – so terms like ‘interlibrary loan’ (ILL) will appear as a permission in a publisher to library licence message but would not have any general application.

ILL also helps to explain one other aspect of the proposed approach. ILL is not really a single permission – it is a whole complex web of permissions, prohibitions and conditions strung together.

These can be expressed

- in a very generic form: permits “ILL”

- or in a very granular form: permits a librarian at institution “A” to make a copy of a defined part of resource “X” in physical (but not digital) form and sending that copy of part of resource “X” to a librarian at another institution “B” – subject to the condition that institution “B” is in the same country as institution “A” – and then the librarian at institution “B” may pass that copy of part of resource “X” to a user – subject to the condition that the user is an employee of institution “B” and is using the copy for academic non-commercial research – and all subject to a condition that the librarian at institution B maintains a record that the copy was made.

An appropriately structured message should be able to handle either the simple or the complex message in exactly the same way. Although still at the proof of concept level, the proposed ‘ONIX for Licences’ message that was tested at the workshop appeared to meet the fundamental requirements of granularity, flexibility and extensibility. There were no fundamental problems identified at the conceptual level.

This does not mean that there are no problems with the approach being proposed. Some of the major ones that were noted included the following.

- There is real concern on the part of librarians that the development of licensing messages would represent the thin end of the wedge in terms of introducing DRM enforcement technology into the relationship among publishers, libraries and library users. It might enable publishers to introduce contract terms which librarians are currently able to resist on the basis that it is technically impossible for them to comply.

- There are concerns on both sides of the argument about the possibility of removing ambiguity from licences: there may be times when deliberate ambiguity in a licence may be advantageous to a successful negotiation.

- There are issues about the canonical licence (and ultimately about liability...
should a system misinterpret a licence term)

None of these, though, are ultimately deal breakers. That the first is a problem is undeniable but will not be contained by the failure to develop a standard message (although the development of such a message may slightly hasten the point when the issue needs to be negotiated). It remains possible to retain ambiguity in a licence message, just as in a paper one but a machine will be unable to interpret the message if the ambiguity is carried forward into a system. And interpretation of the canonical licence terms and issues relating to liability ultimately are themselves matters for negotiation and contractual agreement.

Of perhaps greater concern is that fact the publishers currently have no platforms from which such messages could be sent since few have automated rights and licence management systems. This is true but with a standard to build to and with a market demand to fulfil, this situation could change quite quickly. Equally, the library systems vendors are keen to build to a standard.

The conclusion of the workshop was that there was certainly enough evidence to suggest that a next-stage pilot project would be a worthwhile undertaking (although there are as yet no certain plans in place). Anyone interested in participating in such a pilot should contact Brian Green of EDItEUR: brian@bic.org.uk.

At the same time, in a very different arena, the Music Industry Integrated Identifiers Project (MI3P), a collaboration between the record industry and the music collective rights societies, has been developing global trade standards in the music industry to support online music licence management, including Musical Work License Identifier Standard (MWLI) and standard message suites to support business-to-business licensing. This project also has technical consultancy support from Rightscom.

After a decade, it appears that the era of exchange of rights metadata is finally dawning.