Digital Rights Management: preventing or enabling access?

Based on a paper presented at the 27th UKSG Conference, Manchester, March 2004

In the digital world, access to the ever-increasing amount of published material has never been easier, but it has brought with it a host of new issues and problems. This paper examines some of these, and explores the possibility that digital rights management (DRM) could hold the key to controlling some of the abuses, rather than being seen as a barrier to access. The importance of trust is examined, with the conclusion that whatever models of working may ultimately be established, a trustworthy network and computing environment are going to be essential elements of a functioning online civil society. DRM as we understand it is simply one component of this environment.

MARK BIDE
Rightscom Ltd

Introduction

I am going to consider digital rights management (DRM) from a number of perspectives. To start with, I am going to take an unashamedly commercial view of this subject because that is where it all begins. I will start by positioning digital rights management in its commercial context, by addressing the whole subject of information commerce and the network.

Physical access

In the days when the products of intellectual property industries were physical, the business of getting access to the product created a point of scarcity in the value chain. It was not altogether easy to package content and to get it in front of a public. Users had to have physical proximity to the physical object in order to be able to make use of it.

In the digital world the access problem has now, as we all recognize, simply gone away. Making things public – the business of publishing – is no longer much of a challenge. We now have many millions of new publishers appearing on the World Wide Web, new ones publishing every day. Not all of them, of course, are very *good* publishers, but that may be seen as beside the point. There have always been good and bad publishers.

Not only is publishing things simple, but re-publishing things is very simple too. Re-publishing things that don't belong to you is just as simple as publishing things that do. Proximity to what has been published work now means, essentially, wherever you happen to be. Access is no longer a point of scarcity. Access has never been the only point of scarcity in the content value chain. There are a number of others but I have time to touch on only one of these briefly.

The *authority* of content remains a key added value in the whole area of information, but in the network it is very easy to exploit and manipulate other people's brands, both their individual brands and their corporate brands. It becomes very simple to take a value that somebody else has added and use it yourself.

Legal aspects of access

Copyright has also created a critical point of scarcity in the information value chain. Only the copyright owner can legitimately create points of access, either by doing it themselves or by licensing somebody else to do it. That has never completely stopped piracy in the past and, as we will see later on, physical piracy remains a major issue for the content industries.

However, physical access is not as easy to create as digital access. It is much easier to create access to things in the digital context than it is in the physical one and the spread of digital technology is driving change in the legal environment. We have seen the wonderfully named Digital Millennium Copyright Act and then a whole set of EU copyright directives, which are now coming into law in the UK. We have also seen a completely new approach to copyright enforcement. IFPI have announced a whole rash of copyright enforcement actions being taken against individuals across Europe, in the same way as the RIAA have been doing in the US. If you think about this, it really is unprecedented for copyright actions to be taken against individuals in this way for things that they are doing pretty much in their own homes.

What is clear is that the law is not going to be enough by itself to control piracy. Casual and systematic copying of intellectual property is simply too easy. It is possible sometimes to pursue organized, commercially motivated piracy using the law, but surely it is going to be impossible to take legal action against every user of peer-to-peer networks. I am not going to ask how many of you are users of peer-to-peer networks, but I know that the number of such users in the UK is stupendously large, and that not everyone is going to get taken to court. What is more, technology escalation is going to make it increasingly difficult to take people to court. We are seeing the growth of phenomena like anonymous peer-to-peer, which is going to make it exceedingly difficult to identify who is uploading and downloading content anyway.

Charles Clarke, whom some of you may remember, was the copyright adviser to the publishing industry for many years and he, a long time ago, came up with the statement: 'The answer to the machine is in the machine'. He was talking about photocopying at the time, but fundamentally what he was saying was that we cannot address technology unless we use technology to address it.

Digital rights management

So, does digital rights management provide the possibility of recreating scarcity of access to content in the digital environment, controlling not only access to content, but also its use? Firstly, what are we talking about when we talk about DRM?

I think it is important to recognize that 'rights' in this context does not really mean intellectual property rights (IPR). DRM is about *network* rights management: that is what the 'R' in DRM really stands for. It is about controlling what you can do on a network. To avoid this confusion, I prefer to use the term 'policies' rather than 'rights'. DRM is about controlling digital *policies*. Those policies in part flow from intellectual property rights, but that is not the only – or maybe even the primary – issue that we should be thinking about when we think about DRM. However, I am going to continue, just for the time being at least, to think about DRM from a commercial perspective, because I think it helps us to make sense of the subject.

Digital policy management

DRM essentially has two separate building blocks: one that I am going to call digital policy management and one that I am going to call digital policy enforcement. Digital policy management is about how you manage digital objects and the policies, rights and permissions associated with them. The tools for this are things like persistent association of identifiers, rights and permissions description, rights and permissions administration and the communication protocols that sit round these activities. We have an infrastructural layer here which is about *identification* and *description* – subjects that I am sure are very familiar to you.

Digital policy enforcement

Digital policy enforcement is the technology that you may use to make sure that those policies are enforced, by being implemented in the technology. So they are about enforcing access and usage control. These are things like 'locked boxes', encryption and the monitoring of use, including 'forensic' DRM – finding out what content is being used and in what contexts.

You need digital policy management in order to have digital policy enforcement. So you have to have the infrastructure: essentially a metadata layer on top of which you have the application

(enforcement) layer. Indeed, many different appli-
cations may sit on top of one metadata layer.

Trust-based models

On the other hand, it is important to recognize that
you do not necessarily need to *enforce* digital
policies in order to have the policies in the first
place. You can look to trust-based business models
as an alternative to the use of enforcement. Where
are we seeing those trust-based models? Wherever
enforcement is not necessary because simple
communication of information about the policies is
sufficient. Clearly, the success of such trust-based
models depends on who your customer is and
what the business looks like, but a clear example is
much of the business that publishers currently do
with libraries.

Communication is going to be central to manag-
ing rights on the network. We have to be able to
communicate about rights in a clear and straight-
forward way. We have to be able to make claims
about who controls rights in 'rights statements'.
We have to be able to make proposals in the forms
of 'offer' and 'requests' to use rights. We have to
have 'agreements' over the use of rights and we
have to be able to exchange messages reporting the
use of rights.

All of these depend on accurate and unambig-
uous identification of the content; of what has been
agreed; and of the use to which the content has
been put. So it won't come as a big surprise that
digital rights management depends at its heart on
metadata standards. We cannot operate digital
rights management without clear and unambiguous
metadata standards to support rights management.

Organizationally-mediated trust

So if we can build ourselves a layer of information
to support it, do we need enforcement, even in the
commercial environment? It is clear that for some
types of content, at least for the moment, this may
not be necessary. Many publishers remain to be
convinced that there is any real risk of replacement
of print in digital piracy. In some sectors, such
digital piracy as is taking place has insignificant
economic impact. In other sectors, enforcement
may not be necessary.

However, the migration of STM journals to the
network has been achieved primarily through
organizationally-mediated trust. Who controls the
use of the journals' content? It is the libraries
through their own organizational mediation of
copyright who have made technological copyright
enforcement unnecessary.

Societally-mediated trust

However, at least as things stand, societally-
mediated trust models – ones that we expect
society to manage as opposed to organizations –
don't work. Ask the music industry about what
happens to you if you depend on society to mediate
your trust models and they will tell you! Stephen
King's experience with *Riding the Bullet* is also a
well publicized example. As you will know,
people did stop paying when they were asked to
pay simply on the basis of trust. So, trust in the
network fails when you move from an organiza-
tionally- to a societally-mediated model.

Alternative models for creation of content

Should we, then, perhaps be looking at other
commercial models to support the creation
and dissemination of content? Should we be
asking: is the commercial model that we have
lived with for all these years inappropriate to our
new circumstances and are we going to have to
change it?

We are already seeing a lot of areas where pub-
lishing appears to be moving to a model of pay-
ment for production, rather than payment for use.
'Free to air' television is familiar to us, as is,
increasingly, the concept of open access journals,
but this is happening elsewhere as well. As you
may be aware, commercial educational publishers
are alarmed by what the BBC is proposing in the
publishing of material for schools. There is a big
move towards a production-based rather than a
use-based content economy.

The other idea that has been much proposed has
been a model dependent on payment for services
rather than content. This has been around for
many years as one of the possible alternatives to
the management of content commerce. While
superficially attractive, I have yet to be convinced

that it really works commercially, except perhaps in a limited set of circumstances.

Indirect compensation

One of the other possibilities about which we are hearing a lot are models of *indirect* compensation. There are two slightly different forms of this, mostly depending on which side of the Atlantic you sit on. In Europe, or at least in mainland Europe, there is a tendency to think in terms of *levy systems* which, of course, collect very substantial sums of money in some parts of Europe. Essentially, there is a levy collected on media; the money collected is distributed to the owners of copyright material that has been copied.

In the US there is a movement gathering ground for the compulsory blanket licensing of content, through payments made by consumers to their ISPs, so that when you pay for your broadband connection you are actually going to be paying a blanket licence fee for using content on top of the fee for the technology. The difficulty with these models is firstly that they depend on mechanisms for distribution of the money collected which are not always entirely satisfactory; and, secondly, they tend to divorce *market* mechanisms from the creation and dissemination of content, which may not be a good thing in the end.

Problems of DRM

But if we are not going to adopt alternative commercial models, then can we use DRM to protect models more like those with which we are familiar? Is this a realistic proposition? Well, it is no use pretending that there are not a lot of objections to DRM, of which probably the most significant is that it won't work! Mark Andreessen (the founder of Netscape, who is not someone you can simply ignore when he talks about technology) claims that "If a computer can see it and display it and play it, then it can copy it". So maybe this is not something we can stop. Maybe there is no way forward.

There is an equally valid objection: 'It isn't fair and it won't be acceptable to customers.' I am old enough to remember the days when, if you bought some types of software, you had to put a 'dongle'

in the back of your computer in order to make it run; of course, that whole approach to software protection failed because of customer unwillingness. DRM also has a problem, since it involves the 'hard' codification of 'soft' concepts like fair use or fair dealing. How do you control those very soft concepts like 'substantiality', key to copyright law, in computer code? The simple answer seems to be 'you can't'. So is DRM going to erode exceptions to copyright? There is clearly a *risk* that it does so and clearly there is also a risk that it erodes personal privacy; that is a subject to which I will certainly come back.

Beating back the tide

However, perhaps the biggest single argument is this: are we simply trying to beat back the inevitable tide? Is this simply a case of: we can't get away from it, the network is not going to allow us to do anything about it, and we have got to learn to live with it? So, let us consider what the 'tide' may be that we are dealing with. I do not need to tell you that the music industry is suffering the most enormous volume of digital piracy. So is the movie industry, which is becoming increasingly concerned about the future as bandwidth increases further and further. We now see the movie industry as being in the same place as the record industry was five years ago, in some ways in deep denial over this problem. They think that the solution lies in more draconian law and not in facing the realities of the situation (which is that the law will never be enough).

Piracy also continues to be a major issue in software; it is more than likely that there are at least a few people reading this who at some point have downloaded software that they haven't paid for. We have all of us been involved in casual piracy. It is simply too easy and too straightforward. And some of it certainly feels like fair use. But the statistics show that it really is a problem.

Failure of trust

What we are talking about here is a failure of some of society's trust mechanisms. I want to look at some other examples of failure of trust, because I think these are actually in many ways more telling.

Dear Wells Fargo valued customer!

Please read this important message about security. We are working very hard to protect
our customers against fraud. Your account has been randomly chosen for verification. This is
requested to us to verify that you are the real owner of this account. All you need to do is to
click on the link below. You will see a verification page. Please complete all fields that you will see
and submit the form. You will be redirected to Wells Fargo home page after verification. Please note that if you
don't verify your ownership of account in 24 hours we will block it to protect your money. Thank you.
http://www.wellsfargo.com/verify/

I got this e-mail the other day. The one thing that clearly saved me from responding to it is that I am not a customer of Wells Fargo Bank. However, all the major banks have seen e-mails of this kind. I bank with Barclays and use online banking all the time; Barclays have a large notice on their splash screen saying 'if we send you an e-mail asking for you to do this, it is not from us'. Yet many people are caught.

Dear Friend,
Top of the day to you my friend? It may astonish you to be informally contacted for a pending transaction of this
magnitude more especially since you do not know me personally. The purpose of my introduction is to bring to
bear my present position and the very need for true and solicited help with regards the transaction at hand. I am
Lance Kabade, the personal assistant to Charles Taylor, the former President of Liberia. He has recently
stepped down from power and is presently in asylum in Nigeria.
Well dear friend we need your assistance in transferring some of the money derived from gold excesses into
your account, because the government is making plans to seize all his assets. I have been mandated to deal
with anyone who offer assistance to have this funds transferred to his account overseas.
View these websites: http://www.cnn.com/2003/WORLD/africa/08/11/taylor.warcrimes/index.html
http://www.cnn.com/2003/WORLD/africa/08/11/liberia.1300/index.html
The amount is USD$48 million, in a Security firm Abroad. All that is needed is for me to instruct the company to
transfer the funds to your account, I will need to discuss benefit with you as soon as you make contact. To
indicate your interest, please kindly provide me your direct phone and fax numbers and all relevant information
for me to contact you and to let you know the roles you will play in making this transaction successful. All the
necessary information on how the funds will be collected will be given to you as we make progress.
If this proposal satisfies you, please contact me on phone: + 871 762 91970 and fax: + 871 762 91971
immediately with your full names, telephone and fax numbers to enable me give you the details.
Thanks for your anticipated cooperation.
Best Regards.
Lance Kabade.

Note: Please I want you to reply this mail via lancekab@yahoo.com

---

Here is another approach which many of you will probably have seen, from a man who says he was the personal assistant to Charles Taylor, the former president of Liberia. He is trying to persuade me that if I was only to help him get $48m out of the bank, I would be able to have a large part of it. This scam has been around a long time. I get probably two or three of them a week. Again, people continue to be caught by this.

The MessageLabs SkyScan Anti-Virus service discovered a possible virus or unauthorised code (such as a joke program or trojan) in an email sent to you. The email has now been quarantined and was not delivered. Please read the whole of this email carefully. It explains what has happened to your email, which suspected virus has been caught, and what to do if you need help.
To help identify the quarantined email:
The message recipients were mark.bide@rightscom.com
The message senders were cbabulle@hachette-livre.fr
and they have been notified that they have sent a potential virus. The message title was Re: my data
The message date was Thu, 25 Mar 2004 00:10:42 +0100 The virus or unauthorised code identified in the email is >>> W32/Netsky.P-mm in
Some viruses forge the sender address.

Any of you who have good anti-virus software will have been seeing a lot of these notices recently. I had three or four just like this last night telling me about copies of Netsky that had been caught in the virus trap on the way in to our server. What I find interesting about this is this last statement.

Some viruses forge the sender address and there is a sender address on there. Somebody at Hachette Livre in France appears to have sent me this; I can be pretty certain they were not the sender of this e-mail.

GET YOUR UNIVERSITY DIPLOMA
Do you want a prosperous future, increased earning power more money and the respect of all?
Call this number: 1-917 591 5067 (24 hours)
There are no required tests, classes, books, or interviews!
Get a Bachelors, Masters, MBA, and Doctorate (PhD) diploma!
Receive the benefits and admiration that comes with a diploma!
No one is turned down!
Call Today 1-917 591 5067 (7 days a week)
Confidentiality assured!

Finally, one of the more acceptable bits of spam that got through our spam filter. I haven't shown you some of the bits of spam that get through because I thought they would be too much of a shock at this time in the morning, but here is one that won't surprise you perhaps – although I guess it will horrify you. I could pop out and get myself a doctorate later today. No one is turned down and I don't think they cost very much either.

The importance of trust

So what is the linking factor? I suggest it is the failure of trust. Of course, we are not the sort of people who fall for these things, are we? We do not fall for these sorts of tricks, but 'other people' do.

Some unfortunate woman recently fell for one of those begging letters from Africa to the tune of £40,000. Those who perpetrate this fraud and deception are actually getting more sophisticated in what they do every day and what they are doing is impairing trust, our own trust in the network.

What is this trust thing – what do we need to be able to trust? Well, we have got to be able to trust identity: what is this, or who is this? We have to be able to trust in the authenticity of what it is that we are seeing on the network: is this what or who it is asserted to be? Is this claim that is being made true? We have also got to be able to trust in the channel. We must have secure and dependable – trustworthy – channels of communication if we are going to continue to use the network as we do.

DRM and computer technology

So what does all this have to do with DRM? DRM – in the sense of digital policy enforcement technology – is just a single element of a trusted network and computing environment. The technology at the moment is at a very early stage of development and is still very immature.

We are still nowhere near to understanding how this technology is really going to work in the future. The rights that we want to protect are not only IPRs, but some rights that are much more important to all of us. The right of privacy is an extremely important aspect of this and is paralleled by issues relating to corporate confidentiality. If you look where DRM is moving now, it is moving much more clearly in the direction of corporate confidentiality than it is in the direction of intellectual property rights.

Unless we have a trustworthy network and computing environment, then the network, this absolutely central element of our everyday lives, is going to become increasingly unstable. For how long are we going to be able to continue to use the network to access anything that is of value with confidence, as it increasingly becomes a haven of untrustworthy content and untrustworthy individuals?

Conclusion

The impetus for trusted computing is actually going to come from users and not from the media corporations. It is you and I who are going to be demanding that we have the technology that we now call DRM. This is not about imposing technology solutions, but about fulfilling a requirement that we all have for a network that actually works; consent is absolutely central to that.

The effective protection of intellectual property on the network will be a consequence of trusted computing and not its cause. It is just one element of the creation of a functioning online civil society. Building this is not going to be easy. We are going to have to find ways of dealing both equitably and consensually with issues like fair dealing and privacy in the network environment, just as we have in the physical environment. That is why DRM is going to be important to all of us.

■ **Mark Bide**
Senior Consultant
Rightscom Ltd
10 Leake Street
London SE1 7NN, UK
E-mail: mark.bide@rightscom.com