12th Conference on Computers, Freedom & Privacy
San Francisco, April 16th-19th 2002

Fair Use by Design

Session 3: What DRM can and cannot do….and what it is or isn't doing today

Nic Garnett & Tomas Sander[1]

It is important to keep the issue of DRM in perspective. Whatever the current state of e-commerce development and the technology that supports it, we certainly are not about to enter a world in which all information and entertainment services will be on-line and operate in an environment hermetically sealed by technology. Optical disc technology, for example, will likely remain the dominant medium for audio and video home entertainment for many years to come.

Much of the controversy around the topic of DRM is, in our view, premature or confused. There needs to be a more measured and, above all, informed examination of the likely issues that DRM's eventual importance involves. In this presentation we draw attention to what we consider to be some of the more important issues and questions in the hope that we will contribute some clarity to this area.

The stepping off point is the need to understand that business on-line with information in digital form is a very different process from the information business in traditional forms – an obvious point but one that it would be fair to assume had been overlooked in many of the debates around DRM. Business models and regulatory systems from the old economy aren't per se translatable or even relevant in the new environment.

A second intriguing issue which we flag here for further study as an important contextual feature is what might be called "the digital precision problem". Just as many businesses rely on imprecision to achieve their objectives – legitimately or nefariously – so the implementation of copyright law is equally imprecise. In the UK the copyright law still requires private copiers of copyright material to seek authorization from the rightsholders; no-one does. Collective administration of royalties is in many an extraordinarily imprecise process. No-one, for example, has established an accurate or equitable basis for distributing the enormous revenues collected as levies on copying materials and equipment. Digital technology is very difficult to apply to this kind of vagueness.

There are problems at the conceptual level too. The EU Commission has carefully avoided precision in fashioning the compromises that characterizes European legislation in the area – from the 1992 Rental Directive to last year's Copyright Directive. As is

[1] Nic Garnett is a former Senior Vice President of InterTrust Technologies. Tomas Sander is a member of InterTrust STAR Lab. The views expressed herein are those of the authors alone.

widely recognized, the fair use mechanism in US law falls into roughly the same problem area as far as the application of DRM to copyright materials is concerned.

The precision of digital solutions struggles to co-exist with such concepts and practices; in delivering unimpeachable responses to who gets paid what and when, DRM challenges the essential economic elements of many established business models. Of course, the opposite spin can be put on this: that technology generally and DRM systems in particular cannot match the applied (im)precision of, for example, the fair use mechanism or the way many activities and businesses involving the use of copyright materials are able to continue only because they are beyond the strict enforcement of the law – the latter, of course, a proposition of much broader relevance than copyright.
The third and for us here the most important issue is achieve a better understanding of what we mean when we talk of DRM. We believe it is too early to attempt to develop a generic definition of DRM and we prefer to suggest that focusing analysis on specific systems that have at least some likelihood of being deployed is more appropriate. Being specific about specific DRM systems in our view offers the following possibilities and advantages:

1. It enables us to be more specific as well about the features of each. This in turn facilitates a more objective and useful evaluation of each system in its own right and within a particular commercial, legal or social context.
2. It enables us to better evaluate assertions regarding business/ rights model neutrality of particular DRM systems.
3. It helps in understanding how different systems do or do not work together and how therefore they fit into the overall infrastructure; this understanding is important in developing standards that can advance interoperability. It is also important in identifying bottlenecks or failures within the infrastructure due to overbearing reliance on proprietary systems or anti-competitive deployments
4. It should help in distinguishing systems deployed principally to sustain and protect existing business models and those that are intended to support new business/ rights models. We firmly believe that acceptance of new technology will depend on *all* parties benefiting from what it makes possible.
5. It helps in evaluating in a practical sense what different systems can and cannot do:
    a. what information and rights can they secure and manage?
    b. what rights models can they support?
    c. what business models will they support?
    d. What rights expression language is used?
    e. do they have dynamic rule setting capability?
    f. Can system users be revoked?
    g. Who administers the system?
    h. Who runs the back end and how does it work?
    i. How does the system deal with user and financial information?
    j. What payment system does it use?

These and a host of other questions have to be answered to get any real sense of

how a particular system works.

6. It will help to give more shape to the public debate about the key issues at the intersection of public interest, technology and law. At present the major media conglomerates probably secretly relish the controversy around DRM (in its broad sense) as it adds to their arsenal of excuses for not moving to effectively adopt new technology and to address the profound challenges to existing business models and profitability which it brings
7. In short, it will help to better understand both of threats and opportunities of DRM

To understand the implications of DRM for fair use and copyright law in general, it is not sufficient to argue about rather abstract and fuzzy notions of what DRM is. Rather, it seems important to consider individual DRM technologies, architectures, and implementations and the impact they have on fair use and copyright law. To put some if these ideas to the test we now proceed to examine specific systems and architectures. We then go on to consider the application of the system to the implementation of certain fair use provisions.

DRM Technology

DRM technology is typically based on the concept of the distribution of content in encrypted form. We describe here the basic features of an advanced or "sophisticated" DRM system as developed by InterTrust Technologies.

First, digitized content is encrypted by a packager and typically distributed to consumers, on the Internet, e.g., from a "content server". Rules – commonly referred to as "rights" - which specify how the content can be used are delivered independently from the content. These rights are expressed in a language such as XrML, ODRL and XMCL.. These rights may contain timeouts for how the long the content can be used, to which type of devices the content can be transferred, how often it can played etc.

An important underlying concept is therefore this separation of the rights from the (encrypted) content itself. A user who wishes to use the content, say from his PC, downloads the encrypted content, e.g. from a content server on the Internet. To use the content he will additionally need to obtain the rights and the cryptographic key for decryption of the content from a server. It is essential to understand that within such a system, the content is never made available in the clear and can only be rendered for use by a consumer in accordance with the relevant rights. The other critical feature is that the rights applied to particular content and particular users or classes of users are not static; they can be changed as the content provider sees fit and as the market will support.

A typical commercial transaction looks as follows. A user visits the web site of a web retailer. He purchases a certain content offering, e.g., a subscription to a music service and receives an electronic receipt from the web merchant, that he can then redeem at a DRM server in exchange for the rights and keys the user to access the content.

A user has DRM client software on his machine. This software will decrypt the content and make it available to the user as specified in the rights.

These design principles underlie most of the existing DRM solutions, such as InterTrust's Rights|System and the Microsoft Windows Media Player.

A novel type of architecture which technology of this kind supports is the so-called locker services. Remember that in a DRM system to access content in the protected format the device needs to obtain the encrypted content, the rights and the needed cryptographic keys. A locker is a central depository for the digital rights of a user facilitating this process. A user has an account at the locker service and can access his content potentially from any DRM enabled device that can be online and connect to the locker service (like e.g. PCs, cell phones, PDAs). The key advantage of a locker service is that it enables technically anytime, anywhere access to a user's content. Typically a user logs on to his locker account via a web browser and by typing in his username and password. This architecture is in line with recent trends in computing, such as web services, in which Standards like SOAP have been developed to facilitate interoperability among devices. Typically a user logs on to his locker account via a web browser and by typing in his username and password.

An important implication for fair uses is that using lockers has the potential to reduce the need to make private copies. A user who wishes to access content from a device simply contacts the locker service for downloading the access rights and keys.

Note that a locker may now internally apply a number of policies to grant access and usage rules to users. For example the locker may give a user access to his rights from each device he accesses the locker. A locker may alternatively apply a policy to limit the number of devices from a user may access his content but it doesn't have to.

Novel business models

Electronic distribution enables a number of novel business models, which are impossible to realize in the physical world. Subscription to whole content catalogs becomes technically feasible, e.g., to music catalogs, book catalogs, and movie catalogs. Another example are pay per play/view models, e.g., 10 cents to play a song once, or 10 cents to read an article once. Electronic distribution may also facilitate discriminatory pricing, by e.g. offering basic and premium services for access to content at different prices. Although DRM technology is often described as a limiting technology this might be a misconception. The above examples (and the previous locker example) show that DRM technology can also be an enabling technology for novel ways of accessing content.

Some implications for fair uses

DRM has been criticized for hampering fair use. This discussion suggests otherwise.

There are two extreme positions about DRM. One extreme is that DRM locks up content hermetically simply. The other extreme is that DRM provides “no protection at all”. Both positions start from wrong assumptions and seem to lead to distorted results.

At least in some areas, state-of-the-art DRM systems take fair use considerations directly into account, challenge the presuppositions on which fair use exceptions are based or enable the consumers to use content in novel and more pleasant ways.

Technically a number of fair uses such as for private copying can be accommodated by enabling (rule-based) portability and transferability of rights and keys. This is likely to cover most “normal” private copying activities. Many practical needs for private copying may disappear through technical measures, like enabling portability of digital content. Locker constructions demonstrate clearly that the key concept is not copying, but access to rights. In a digital environment where DRM rights locker architectures enable consumers to use their content at anytime from any device at any location, private copying may become much less relevant.

Many fair uses such as citation and parody will not be affected by DRM at all. A critic can still quote from an ebook, by retyping paragraphs. DRM does not (and can not) technically lock up content a 100%. An artist wishing to make, say a patchwork of sound or video recordings can always rerecord the analog output of a rendering device. Secondly for many years to come digital and traditional distribution mechanisms will coexist giving parties (say artists) the ability to choose via which medium they wish to access content. Also other fair uses, like copying for archival uses do not seem to present any major technical challenges.

DRM technology can also be used to support fair uses in a novel way. For example, an “educational rights locker” operated by educational institutions could be used to grant access rights to students. Public interest issues should be reevaluated in light of the constraints and the benefits of this new technology.
One of the most important effects of DRM is, that it removes vagueness. We called earlier in the text the “digital precision problem”. The main challenge is that parties need to agree on rules of usage in areas that were previously left vague, e.g. publishers and schools.

Restrictions concerning private copying and other fair uses in DRM technology are today mostly based on (reasonable) risk management requirements. How much protection and security measures are exactly necessary to create commercially viable systems is unknown. Gaining practical, real-life experiences with DRM systems will allow us in the future to address the real issues around fair use and public interest issues instead of the currently perceived one.

We recognize that we have delivered here a set of abstract propositions regarding the capabilities of DRM and have not addressed the obvious issues such as how DRM

technology by media conglomerates; how public interest rights lockers would be structured and administered; how invasive of consumers' privacy will the technology be; the co-existence of traditional and DRM enabled business models.

Our focus here has been to provide some practical clarification from a technical perspective of what is meant by DRM. We believe that only with a proper understanding of the basics of the technology can we begin to address the broader, critical deployment issues. We are not asserting that DRM technology is a neutral component of the electronic market place structure but we do urge the development of general and objective understanding of what particular DRM systems can and cannot do.