Digital Rights Management
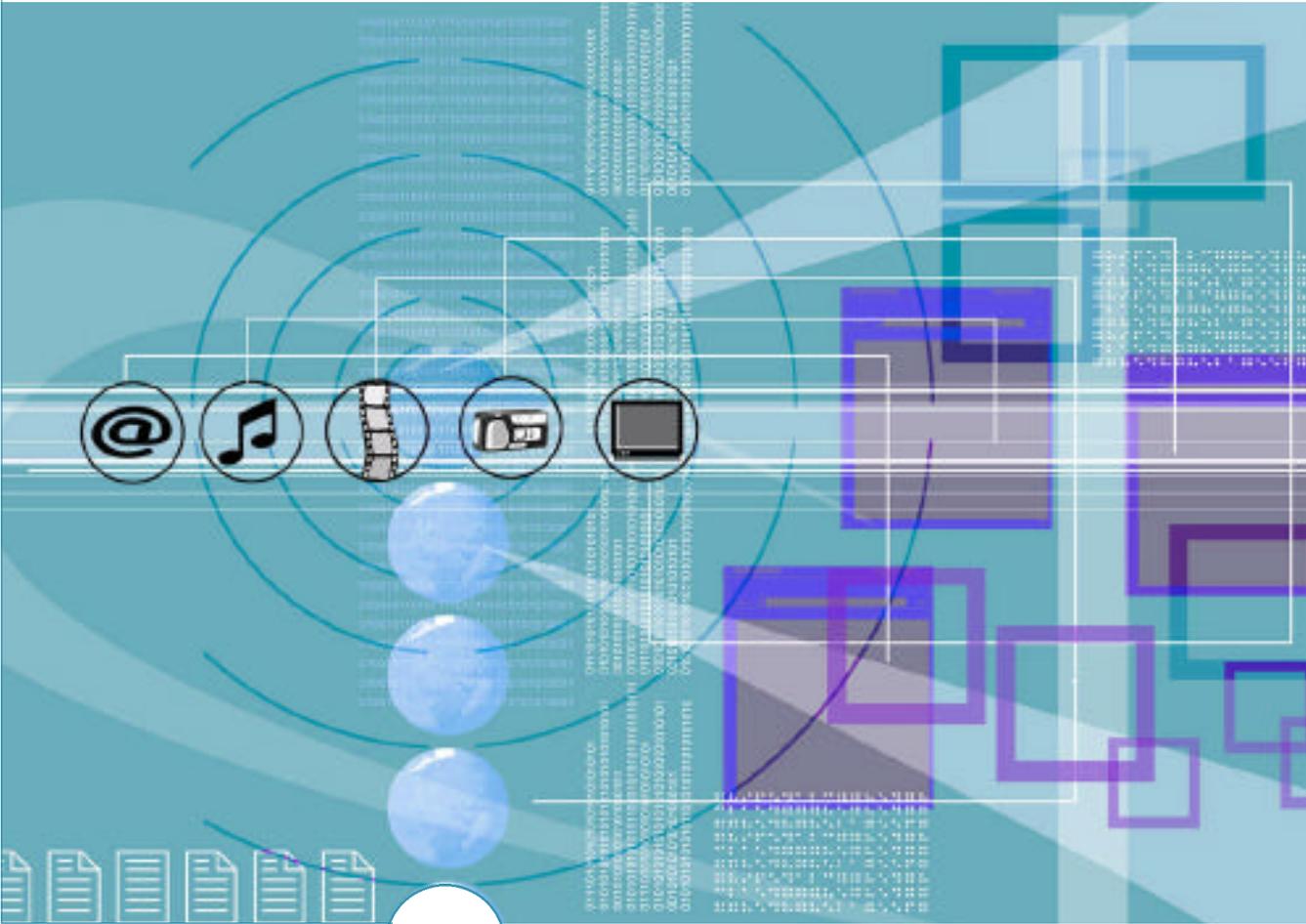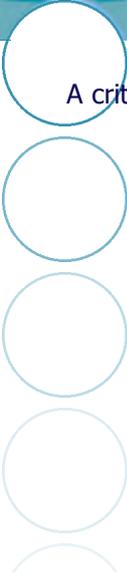
MISSING LINKS IN THE BROADBAND VALUE CHAIN

A critical snapshot of the DRM debate and the ongoing quest for solutions

BSG

**Broadband
Stakeholder
Group**

Contents

Foreword

Last week 17-year old Dan was chatting to some mates about football, clubbing and their favourite DJs. One of them had just heard that Dr.M was releasing a new track called 'Where da money?' so later that night, Dan logged on and searched for the track. Since he was on his dad's PC, he tried the legit sites first. He found the track alright, but didn't fancy taking out a subscription, the only option on the first few sites. So he carried on searching before finally stumbling on a service that offered a straight download, and they had the new track. However, he didn't have a credit card and found he couldn't pay through his pre-paid mobile phone. That depressed Dan, not because he couldn't get hold of the track - he knew how to do that for free - but because he couldn't see how he was ever going to make money from the cool digital stuff he was working on with his mates.

Where does Digital Rights Management (DRM) fit into all this? In some form, DRM is necessary at every stage in the digital value chain. It provides the basis for all transactions for authorised use of content. DRM tools and systems – of which there are a number already on the market – offer powerful solutions. But DRM is not the panacea. DRM solutions are only as good as the legal and business framework they support.

This report examines the issues surrounding DRM and highlights those things that are impeding its development. Two things stand out – the lack of micro-payment systems and the ongoing negotiations over new business models. These are holding back the deployment of DRM solutions and the delivery of content through broadband. They present major challenges to the finance sector and the numerous stakeholders in the digital value chain.

For DRM itself, agreeing standards remains a major task. Delivering the interoperability which consumers are demanding will require agreement at international level across all the different industry sectors. Government will have a key role in this, both through the standards agencies and as a major provider of public services, all of which should deploy the same DRM standards as are adopted by the private sector.

The report even addresses the thorny issue of copyright exceptions and DRM's role and limitations in facilitating access. Crucially in this area, DRM cannot solve legal ambiguities and there is a clear message to Government that accommodating exceptions may require both online and offline solutions and that they all carry costs.

I would like to thank all those who have contributed to this report, the result of a few months of intensive, and at times heated research, debate and discussion. In particular I would like to pay tribute to Nic Garnett, drafted in from The Simkins Partnership to write the report. He has done sterling work in a very short time. We should also thank the DTI for taking on this secondment and enabling this report to be produced. I hope that this will help inform the debate on DRM and the issues surrounding it and accelerate the quest for solutions, soon enough that my friend Dan and his mates have a chance to make some money from their cool digital 'stuff'.

Dominic McGonigal
Chair
BSG DRM Group

Executive summary

The huge popularity of Napster and other file sharing technologies has shown that access to content is an important driver of online consumer activity. Rapid consumer broadband take-up in the UK is heavily dependent on the availability of content. The critical question is how to ensure the wide availability of content while maintaining the rights of content providers in a manner consistent with established principles of intellectual property.

Does digital rights management (DRM) provide the answer? Is the availability of DRM tools and systems the key to enabling the kind of online content services and systems that will boost broadband take-up by consumers? This report and its conclusions are the result of discussions with numerous stakeholders in the digital value chain by the BSG DRM Group aimed at answering those questions.

There is no doubt that the use of DRM tools and systems is growing in importance in a multitude of contexts - in business to business (B2B) applications, in business to consumer (B2C) applications; in both private and public sector applications; across different platforms; and for many kinds of content. As a result, they are becoming more advanced and more efficient. DRM tools and systems have the potential to radically improve digital content management as well as to resolve some of the stresses under which digital technology has placed traditional rights protection processes.

Having said this, it is important to emphasise that DRM should not be seen as a complete substitute for traditional methods of content and rights protection. Nor can it be seen as providing by any means the entire solution for the commercialisation and automation of online content services.

The report's conclusion is that while DRM is an essential part of the overall solution, it is not the single panacea. DRM tools and systems provide powerful functions but they are also dependent on the business and legal environment in which they operate. Essential elements for the effective deployment of DRM systems include interoperability in metadata and rights expression, e-payment systems, business models and the legal framework to support them.

E-payment and billing systems

For content providers to explore fully the possibilities of online commerce, they have to be able to innovate in terms of their business models. They should not be confined within structures predicated by the capacities of existing payment systems. It is, of course, for the individual content provider to decide how to commercialise its content and rights and it is equally true that the kind of investment required to establish an effective e-payment and billing system has to be justified by clear market demand. However, it is important to recognise the limitations of existing systems. The current payment systems do not cater adequately for micro-payments necessary for many new business models, for certain consumer sectors and for the interoperability demanded by consumers across different platforms. Correcting this situation could offer tremendous opportunities for developing innovative commercial content services, providing a "win-win" UK scenario for both its broadband strategy and its world leading content industries.

Standardisation

DRM tools and systems of wide application comprise highly sophisticated technologies which in turn require enormous resources to develop, the kind of resources that, in practice, only very big enterprises can muster. These enterprises need a guaranteed return on their investment to justify the application of the resources; they need to own what they invent and develop. At the same time, these technologies and their related components such as Rights Expression Languages (REL) are called upon to perform many different tasks across a wide variety of platforms and in relation to a very diverse range of content. DRM tools and systems have to achieve a satisfactory level of interoperability if they are to provide a generally usable mechanism.

These potentially conflicting propositions have to be reconciled through market supported standard setting processes. Encouragingly, this has been recognised by most of the major constituents and a number of important standardisation initiatives are under way. Having said that, standardisation processes are complex and prone to delays particularly where major existing proprietary interests are involved. It is therefore essential for government to actively support market-based standardisation, based on up to date knowledge of relevant processes. There should also be constant vigilance to avoid a single proprietary system, where it becomes the dominant system for a particular platform, being used to undermine open standardisation or worse, to promote the system proprietor to the position of the gate-keeper for content management conducted on that platform.

Piracy

File sharing technologies which facilitate the direct infringement of copyright have the potential to destroy important areas of creative, cultural activity: shrinking rosters of creative talent in the music industry bear compelling witness to this fact. The latest figures from CNET show that Kazaa Media Desktop, the most popular file-sharing software, has been downloaded a staggering 225 million times and at an ongoing rate of 2.5 million downloads per week; Morpheus, the number two system has registered a further 111 million downloads.

DRM does not in itself offer a solution to this problem particularly as the bulk of the content industries' business is still conducted off-line in formats that are difficult to protect[1]. Urgent action is therefore required by government to update existing rights enforcement measures to provide an effective response to this situation. DRM can facilitate new business models but there should be no illusion that, however innovative the legitimate offerings, they can beat that most obvious form of market distortion: piracy. There is no realistic possibility of "competing with free".

[1] The DVD Video format while still relatively secure was early on the subject of an attack on its encryption system; attempts by the music industry to introduce copy control technology for CDs has met with negative reactions from consumers.

Public sector

This is the first report of its kind to address the use of DRM in the public sector.
It does so for three reasons. First, public administration and public services will have
a major impact on the take-up of broadband services both in terms of their own needs
and their interface with the public. DRM has the potential to bring major innovation
and efficiencies in both these dimensions. Secondly, certain public services such as
education and libraries, in adopting DRM-enabled systems, can provide primary testing
grounds for DRM as a means for fairly and efficiently implementing the terms agreed by
rights holders and users in respect of certain public interest exceptions and limitations
to copyright. Thirdly, many public service institutions have there own enterprises in
packaging and selling content: DRM enabled systems can be deployed to distinguish
between these and other uses of third party content covered by limitations and
exceptions to copyright.

Recommendations

In response to these and other issues the BSG DRM Group has drawn up the following recommendations:

1. **DRM tools and systems should be regarded as falling squarely within the inventory of online security measures.** In devising ICT security policy and responding to initiatives in this area at the European level Government should ensure that DRM is considered as part of the mainstream security definition rather than as sub set of mechanisms for enforcing intellectual property rights.

2. **Government should urgently consider the formulation and adoption of "effective measures for enforcing intellectual property rights", in line with the requirements of the TRIPS Agreement, to deal with online piracy.** It should also, along with industry, take every opportunity, including consultations on the EU Proposal for an Enforcement Directive[2] to press the case for such measures at the international level.

3. **The UK content industries should jointly commission a study into the application of the emerging rights data dictionaries and rights expression languages to the licensing and management of copyright materials.** Particular attention should be paid to the relationship with traditional systems of rights administration and whether the emerging languages are adequate for dealing with complex rights transactions at the wholesale level - the area of "contract expression languages". Consideration should also be given to the use of rights expression languages in public sector applications of DRM tools and systems and whether these give rise to any particular needs in addition to those already identified by the private sector.

4. **Government should actively promote the development and promulgation of global DRM-related standards.** The standards including those of metadata, rights data dictionaries and rights expression languages should be established by the private sector through existing international standards bodies, such as ISO. Government should also actively engage with the European Commission to ensure that the latter adopts a similarly pro-active agenda for the development of global standards.

5. **Government should commission an in-depth study into the area of electronic payment and billing systems.** It should ascertain the scope of application of existing systems, find out what content providers need from e-payment systems and assess the prospects for development of existing and new systems to meet the demands of the various consumer sectors, markets and business models.

[2]COM(2003)46 final; Brussels, 30th January 2003

6. **The UK content industries and public sector beneficiaries of copyright exceptions (such as libraries and education) should work together to create frameworks for use of content, employing DRM systems to enforce the agreed scope and terms of use.** Government should facilitate definition of the complex issues related with this proposition.

7. **The UK content industries should take the lead in addressing relevant consumer confidence-building measures through establishing codes of practice.** Within the bounds of competition regulation, areas to be covered by these codes could include data protection; technical support and back up services; licence revocation; service and product guarantees; charge back and return mechanisms; alternative dispute resolution.

8. **The Government should implement a number of pilot public service broadband offerings, deploying DRM applications and e-payment systems.**

9. **The BSG should conduct an international review of the impact of legitimate online content services on the take-up and use of broadband.** Particular emphasis should be placed on studying rights management and payment systems used in the delivery of these services.

10. **The BSG should bring together the various stakeholders in the digital value chain to explore new business models.**

11. **Industry and government should work together to bring relevant information about DRM and related elements of the online content service infrastructure to content and service providers, to their customers, to government and other public institutions.**

Introduction

The Broadband Stakeholder Group (BSG) identified early on that content would be an essential driver for the take up of broadband by consumers and businesses. The availability of Digital Rights Management (DRM) tools and systems[3] has increasingly been seen as a key to enabling content services on broadband. Recognising this, the BSG set up the DRM group to examine the principal issues connected with DRM. In so doing the BSG DRM Group would assist in advancing a key priority of the Broadband Stakeholder Group:

> "...to continue to accelerate the adoption of broadband services where they are available making them a "must have" for individuals, businesses and Government organisations alike. The development of a dynamic, competitive, sustainable market is a critical prerequisite for releasing new investment funds for the future."[4]

The overall task of the BSG is to advise the government on the development and implementation of a strategy to enable the UK to meet the government's target to have the most extensive and competitive broadband market in the G7 by 2005. Two important principles govern the approach of the BSG to its task. The first is that "the BSG continues to believe that broadband has real potential to accelerate the five key drivers of economic growth: enterprise; innovation; competition; investment and skills".[5] The second is that "the broadband journey will be market driven but government will need to proactively intervene when the market will not deliver either permanently or in the time scales required by the political agenda".[6]

The UK broadband market is developing rapidly[7]:

72% of the UK has access to a mass-market broadband solution - that is one that is targeted at residential or small business users. Although coverage remains concentrated around areas of high population density.

8% of households with access to broadband have now taken up broadband service.

By May 2003, there were some 2 million broadband subscribers,[8] up from around 600,000 in May 2002.

---

[3]DRM can be understood as the application of trusted computing tools and systems to all forms of content for the purpose of authorising the occurrence of specific events in relation to that content as requested by an authenticated user. For this to occur, the content has to be expressed through a digital format or formats compatible with the selected tools and systems and/ or reside within a compatible processing environment throughout the period during which the authorisation is active.

[4]Keith Todd, Introduction to BSG 2nd Annual Report, November 2002

[5]Idem, p.5

[6]Idem, p.5

[7]Idem, p.6

[8]This figure includes residential and SME subscribers to ADSL, cable modem, fixed wireless and satellite services and services provided via unbundled local loops. It does not include leased lines: See generally: www.oftel.gov.uk/publications/internet/internet_brief/broad0403.htm

The objectives of this report

While this report[9] is produced to contribute substantively to the work of the BSG, it should also serve to improve general knowledge and understanding of DRM and of the key issues related to its development and deployment. Hopefully, it will also serve as a valuable information resource for a wide range of content providers and content service providers as to the current issues and trends in the field of DRM; the emerging standards in areas such as Rights Expression Languages (RELs); the critical commercial elements – such as electronic payment and billing systems – which form part of an overall e-commerce system. There is no readily accessible resource of this kind available at present, one that can have practical effect in helping to facilitate better understanding and thus more efficient negotiating through the relevant value chains.[10]

The scope and focus of the report

The approach of the Group has been to focus on the role of DRM as an element of the broadband take-up strategy required to implement the government's agenda. The approach has therefore largely assumed the importance of content service push as a key factor of the take-up strategy although it has considered the impact of consumer pull.

As is explained in the following section, this report takes a broad-based approach to DRM both in terms of exploring the contexts in which DRM tools and systems are used and in relation to the content and uses to which it is applied. It is important to underline however that, with the exception of one area, this report, in examining the operational and contextual aspects of DRM deployment, focuses on its use in the business to consumer dimension of digital value chains. (The one area of exception is that of the use of DRM in the public sector although here no particular application is considered in detail.) This emphasis should not obscure the fact that there are a growing number of uses to which DRM tools and systems can be applied in the workplace and the business to business environment: controlling access to digital assets, controlling documentation processes and work flow, implementing corporate policies with regard to customer relationship management; controlling interaction with other businesses and distribution of digital products.[11] In these contexts the rights issues that have to be managed can be considerably more complex and detailed than is the norm in the business to consumer dimension of the digital value chain.

[9]The report is the product of the deliberations of the BSG DRM Group over a period of approximately nine months, from July 2002 to May 2003.

[10]See Bill Rosenblatt, Digital Rights Management (John Wiley & Sons, 2001); Gordon E Lyon, A Quick reference List of DRM Standards & Organisations (NIST, October 2002); Bill Rosenblatt, DRM Watch: www.drmwatch.com

[11]For further information, see Bill Rosenblatt and Gail Dykstra, Integrating Content Management with Digital Rights Management; May 2003. Available from www.giantstepsmts.com

BSG

Headline issues

A broad-based approach

This report has adopted a broad-based approach to its subject. While the report's focus is DRM, it addresses a range of topics connected with the management of digital content in general as well as a number of the other major issues content providers will face in that context.

A common perception of DRM systems is that they are unitary technical systems used not only for protecting commercially distributed content against unauthorised use but also for providing the complete set of mechanisms required for automated commerce in digital content. Accordingly, the term DRM has been variously applied, separately or collectively, to copy control/ limitation mechanisms, access control mechanisms, watermarking and fingerprinting systems, metadata systems and rights expression languages – even, in some cases, to electronic payment systems and automated accounting systems.

DRM is not simply about content protection and the management of rights nor is it a complete solution for e-commerce in digital content. A better way to think of it is as the application of certain technical tools and systems to meet specific needs utilised in any digital content management process be it commercial, non-commercial or a combination of the two. (Digital content management as used here is to be understood as referring to any processes of storing, retrieving, transmitting and using digitally expressed content employing tools and systems conducive to the efficient use of such content in any context.) This report aims to describe the broad context of digital content management, to be clear about the function and scope of DRM and to show how the DRM component is placed in relation to the other essential components of the digital content management infrastructure.

The scope and limitations of DRM

It is important to be clear about the scope of application and the limitations of DRM tools and systems. This plays out in two different ways.

First, content providers have received a lot of criticism for their alleged reluctance to venture online and build out new digital content business models based on the availability of DRM tools and systems. As this report will show, while there are a number of developed DRM systems available, other essential elements of the e-commerce infrastructure are not yet in place and cannot in any event be the responsibility of the content providers to provide. E-payment and billing systems are an obvious example of this.

Secondly, the access and usage controls that DRM tools and systems make possible are subject to obvious limitations. The tools and systems are constantly under threat, if not attack, from hackers. More fundamentally, they cannot encompass the entire linear content process from creation to reception because any form of content which is directly perceivable in an analogue form - audio, video - can be copied and re-used from that point.[12]

---

[12] See on this Bruce Schneier, Secrets & Lies (John Wiley & Sons, 2000); Ross Anderson, Security Engineering (John Wiley & Sons, 2001)

In short, DRM is not the absolute proposition that many commentators would suggest it is. DRM tools and systems cannot create a hermetically sealed world for the deployment of content and nor by the same token are they a complete replacement for traditional forms of rights protection. Given the inherent limitations of DRM tools and systems, it is their interrelationship with the various elements of the overall infrastructure which ultimately govern their relative efficiency and of the system as a whole.

Conclusion: DRM will not provide a single generic solution to digital content management. The key to enabling digital content lies in a range of DRM tools and solutions, combined with new business models, effective legislation and enforcement measures.

Interoperability, integration, usability and scalability

For DRM tools and systems to provide real support for the development of legitimate content services, attractive to consumers, they will ultimately need to function seamlessly across the variety of platforms – PCs, PDAs, mobile phones, set top boxes – that consumers will use to access the services. The technical interoperability both of DRM tools and systems and the other components of the e-commerce infrastructure is essential to guarantee the operational and commercial interoperability of services and platforms. The tools and systems will have to be scaleable in the context within which they are deployed, being essentially commoditised and invisible within the operating environment in which they are used. They will have to support consumer interfaces that are readily useable: the technology must not constitute a barrier to the user experience. Finally the tools and systems used must be capable of integrating with the existing rights management infrastructure because the DRM tools and systems in their own right do not provide the functions that, for example, collective administration processes traditionally provide.

Trust and security

The growing automation of commerce through the use of computing technology and the internet means that increasing reliance is placed on machine based web services to not only implement transactions but in effect to negotiate them. Machines have to talk to each other and they have to trust each other. Similarly, as individuals interact increasingly with each other and with private and public sector institutions via computers, so they need assurance that once out there in the "internet cloud" they can retain their privacy and protection for their assets. For the countless manifestations of these needs trusted computing systems are required. Trust in this context means essentially being able to predict with total accuracy the outcome of a particular process conducted by the machine.

DRM represents the application of trusted computing tools and systems to the task of digital content management. The notion that DRM is a particular species of technical protection mechanism created for copyright enforcement is neither valid nor helpful.

DRM tools and systems manage bits in essentially identical fashion irrespective of what they represent: music, personal data, top secret communications; notational currency (e-money). From a regulatory point of view therefore DRM systems should be treated in the same way unless there is a particularly compelling reason to do otherwise. Thus if a particular regime for the application of trusted computing (DRM) tools and systems is decreed for content traditionally covered by, say, intellectual property rights, there has to be a cogent rationale for differentiating the regime from that used for dealing with a notational currency DRM system. Deviation from the default has to be justified and the consequences have to be carefully weighed. There also has to be a carefully constructed mechanism for expressing and implementing the features of that particular regime.

In short, DRM tools and systems are simply one example of mainstream online security technologies.

In an important article published in October 2002, The Economist offered the following observation:

"Digital security has been growing in importance for years as more and more aspects of business and personal life have come to depend on computers. Computing, in short, is in the midst of a transition from an optional tool to a ubiquitous utility. And people expect utilities to be reliable. One definition of a utility, indeed, is a service that is so reliable that people notice it only when it does not work........One of the many prerequisites for computing to become a utility is adequate security. It is dangerous to entrust your company, your personal information or indeed your life to a system that is full of security holes. As a result, the problem of securing computers and networks, which used to matter only to a handful of system administrators, has become of far more widespread concern."[13]

In January 2003 the Council of the Europe issued a Resolution on security in the ICT sector. It invited member States to:

- promote security as an essential component in public and private governance, in particular by encouraging assignment of responsibilities;

- provide for appropriate education and vocational training, as well as awareness-raising, particularly among young people, to security issues;

- take adequate measures to prevent and respond to security incidents, in particular through:

the continuous improvement of the identification and assessment of security problems and the application of appropriate controls;

the establishment of effective ways of communicating the need for action to all stakeholders by reinforcing the dialogue at European and national levels and, where appropriate, international levels in particular with those supplying information society technology and services;

[13]Securing the Cloud, The Economist, 24th October 2002

addressing appropriate information exchange corresponding
to the needs of society to remain informed on good practices
related to security;

- encourage cooperation and partnerships between academia and enterprises
to provide secure technologies and services and to encourage development
of recognised standards.

This Resolution was followed in February 2003 by the publication of an EU Commission Proposal to establish a European Network and Information Security Agency.[14]

Conclusion: While the required levels of security may vary between different types of digital data – music files, financial transactions, health records – the underlying security systems are essentially the same. Each system must be able to guarantee the level of security required for a particular service. The legal protection and regulatory treatment applied to those security systems should therefore be generic, not linked solely to the data type involved.

Recommendation: DRM tools and systems should be regarded as falling squarely within the inventory of online security requirements. In devising ICT security policy and responding to initiatives in this area at the European level Government should ensure that DRM is considered as part of the mainstream security definition rather than as sub set of mechanisms for enforcing intellectual property rights

Time Line: Now and ongoing

Piracy

In assessing the relationship between the availability of online content services and broadband take-up an obvious question can be posed: if consumer broadband take-up is limited when there is wide availability of free content, courtesy of, for example, file sharing technologies, why should the introduction of technologies ushering in a new internet age of controlled content access and use promote wider broadband use?

There are a number of equally obvious responses to this. The first is that broadband take up should not be advanced at the expense of content providers. The UK has long enjoyed a position as one of the world's leading sources of content, a position which should in no way be compromised to facilitate broadband expansion. Broadband is, after all, a means to the end of enhancing the competitiveness of the UK in the Information Society, not an end in itself.

Secondly, in the short to medium term, legitimate digital content services will, with the right drivers, come to form an important part of integrated service offerings appealing to the demographic with decision making power over broadband take up. File sharers do not pay for the content they consume and nor, for the most part, do they pay for the infrastructure they use.

[14]COM(2003)63 final

The overriding justification for commercial digital content management however is that whatever the growth rate of broadband, uncontrolled illicit content distribution has the potential to destroy large parts of the cultural industries. Without the ongoing creative output of these industries the broadband offering, for consumers, will be extremely limited. The music industry which for the last few years has borne the brunt of the negative aspects of the digital revolution is undergoing a difficult transition. Publishers are already having to deal with extensive online piracy due to the ready availability of cheap and efficient OCR technology. The film and games industries will be similarly challenged as bandwidth increases. Reducing unauthorised distribution and use of content is therefore a first priority.

At the same time, the use of file-sharing software by consumers is growing at astonishing rates. The latest figures from CNET on the top downloads of consumer software show that the Kazaa Media Desktop, the leading file sharing software is currently being downloaded at a rate of 3 million downloads per week , a rate which is five times higher than the next most popular software, the ICQ instant messaging client. The same source reveals that the Kazaa software has been downloaded a staggering 250 million times since it was introduced. Morpheus, the second most popular file sharing software, based on the open source Gnutella technology, has registered a further 113 million downloads.

These figures speak for themselves. And yet neither government nor the law seems as yet ready to provide any effective response to the massive threat this phenomenon poses. To advocate that content providers pursue the individuals using this software to commit acts of piracy is simply unrealistic given the scale of the problem – even were it possible to discover what individuals do in the privacy of their own homes, the numbers of infringers are simply too great. It is therefore particularly troubling to see on the one hand a court in California absolving the providers of file sharing technology from liability (although the decision at first instance is to be appealed)[15] and on the other to note the failure of the European Commission to squarely address the problem in its recent proposal for an Enforcement Directive.

Online piracy is a new problem. While there are a number of profiteers taking advantage of this new trend, it is primarily a social phenomenon, being practised by ordinary citizens with the necessary hardware and network connection from the privacy of their own home. New measures are needed for a new problem. In looking for the solution regard must be had to the principles of trust and security outlined in the preceding section. Traditional forms of piracy have been long treated as criminal activities; the new forms of piracy should be treated in the same way, that is as instances of computer crime which threaten to undermine the social and commercial fabric of online activity.

Recommendation: Government should urgently consider the formulation and adoption of "effective measures for enforcing intellectual property rights" in line with the requirements of the TRIPS Agreement to deal with online piracy. It should also, along with industry, take every opportunity, including consultations on the EU Proposal for an Enforcement Directive[16] to press the case for such measures at the international level.

Time Line: Ongoing

---

[15]MGM v. Grokster; US District Court, Central District of California; 25th April 2003 case

[16]COM(2003)46 final; Brussels, 30th January 2003

The importance of a UK initiative

The question here is whether, given the global reach of the internet and of e-commerce more generally as well as the establishment of regulation on a European basis, a report such as this and the recommendations it contains can have any real value beyond the particular needs of the BSG.

There are numerous reasons for responding affirmatively. The UK enjoys an important middle location between the US and Europe on so many issues – political, strategic, and economic. Technology is another area, particularly technology for providing means to facilitate and set the terms for e-commerce. The UK economy is intricately and principally linked with the US economy while its regulatory framework is governed increasingly by the EU. The UK is therefore uniquely positioned to analyse the interaction of technology, economics and law that lie at the heart of DRM based systems.

It is also important for the UK to maintain its leadership in the provision of content and services, all of which will rely increasingly on the use of sophisticated DRM tools and systems. The UK has been for many years, for example, the source of a very large proportion of the world's repertoire of recorded music and is a world leader in writing computer games. Having access to efficient DRM based online systems therefore becomes essential to maintaining this position.

A third consideration, again very much part of the government's overall strategy for broadband technology, is the use of DRM enabled systems in the public sector. This report is the first of its kind to deal with the use of DRM services in both the commercial and public sectors in an integrated fashion. It also highlights the opportunity for ground breaking research into the use of DRM enabled systems to implement public interest provisions of copyright law.

Current trends

Services delivering entertainment and educational content will play an increasingly important role in both consumer and public sector take-up of broadband. DRM tools and systems for such services have been available for several years but it is only now that critical mass is being achieved in terms of bandwidth and connectivity to justify the investment required to bring commercially viable services into being.

The picture is patchy at present with services varying as to their availability across different platforms and across different content types. Additionally, there is still a great deal of searching going on for commercially viable business models, a task complicated by the lack of information about markets, demand and consumer practices. As with a number of issues dealt with in this report, the chicken and egg conundrum is very much part of the current scenario. The costs and risks of launching online content services that are not assured of a ready market are daunting.

Business model and value chain innovation are governed by a number of factors including:

- Business and consumer demand

- Transition from legacy systems and formats

- Bandwidth

- DRM capability

- Availability of commerce infrastructure components
  e.g. billing and payment mechanisms

- Established value chain margins

- Availability of reliable information as to consumer practices

- Regulation

- Corporate culture and the ability to change[17]

Of these, value chain margins are of particular importance to content providers and service providers alike. The coming together of established content industries with the communications industries through the medium of technology can be likened to the interaction of tectonic plates, creating a deeply unstable landscape at present. Furthermore industries which were previously 'self-contained' now share value chains with related or even competing sources of content, a process compounded of course by digital convergence. Broadband service providers, content providing conglomerates and technology interests are working to stake out the new environment according to their respective commercial imperatives. The expectations are high, the complexities substantial.

[17]Cf. C. Christensen: The Innovator's Dilemma
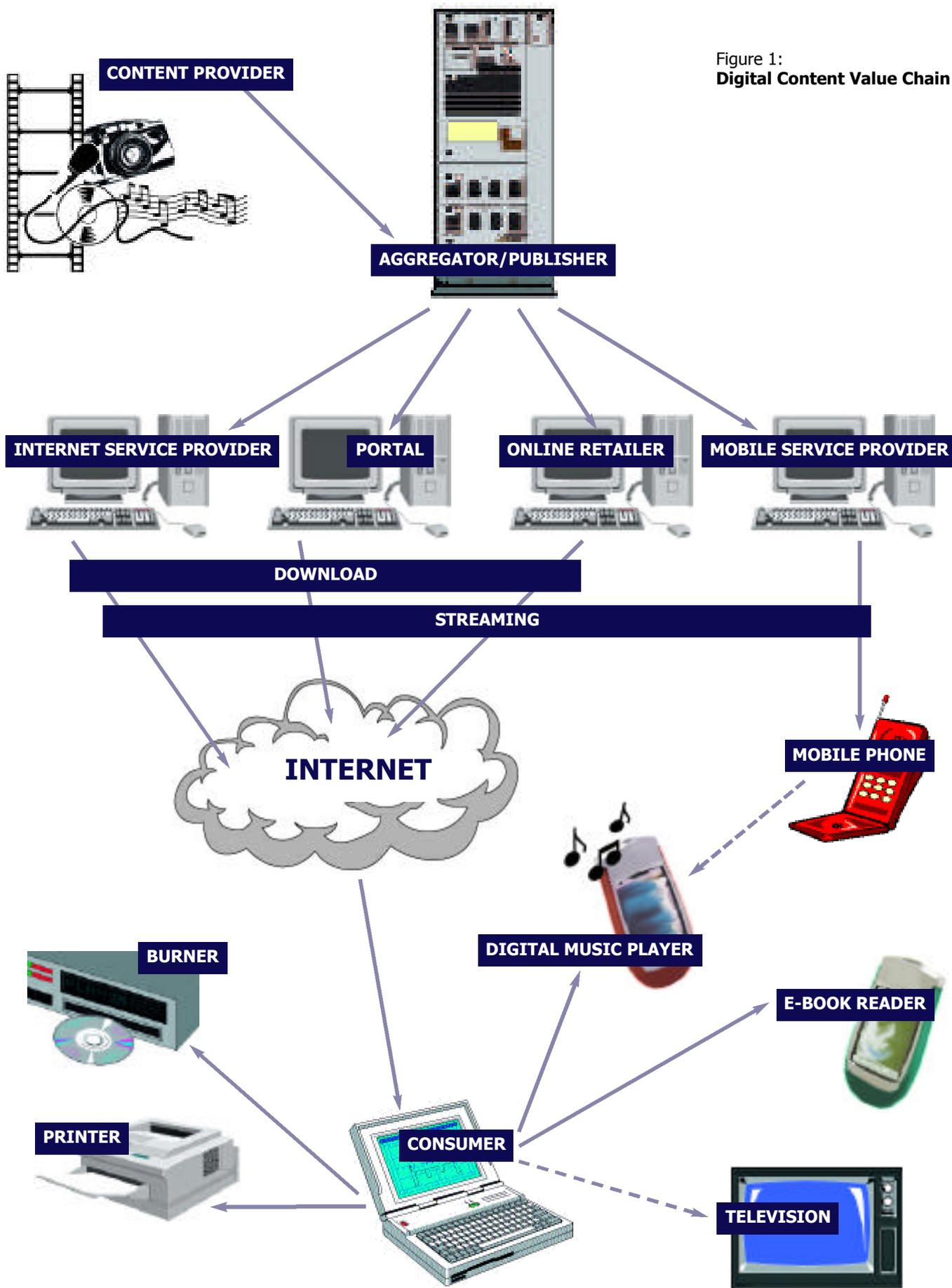
Figure 1:
Digital Content Value Chain

CONTENT PROVIDER

AGGREGATOR/PUBLISHER

INTERNET SERVICE PROVIDER   PORTAL   ONLINE RETAILER   MOBILE SERVICE PROVIDER

DOWNLOAD

STREAMING

INTERNET

MOBILE PHONE

BURNER

DIGITAL MUSIC PLAYER

E-BOOK READER

PRINTER

CONSUMER

TELEVISION

Figure 1 represents a basic, composite digital value chain, beginning with the content provider and ending with the various functions available to the end user (consumer) depending on the form of content and the rendering device used – a digital music player, a television, a printer etc. The complexities and the responsibilities of the various participants in the value chain require further explanation, however.

At the present time, the role of the aggregator/publisher is central to the entire chain. OD2, the leading European music aggregator, describes its functions by reference to three basic components. The first component is the part that the consumer sees, termed the content platform. The content platform is hosted by a number of different third party service providers in various territories and so the content platform has to have multi-portal, multi-lingual and multi-currency capability. The end user connects with the OD2 service through a portal, ISP or online retailer and the service as it is offered to the end user usually carries the brand of that connection point. Behind the scenes however, it is OD2 which is providing the management tools which enables the ISP to establish the front end with its own brand, user interface and pricing rules. The payment system until now has involved a payment by the end user to OD2 using a credit card; it is likely that in some cases payment can be integrated with the billing system of the service provider. In this way, charges for the content would be aggregated and billed to the end user via an account with the service provider.

The second element of the OD2 system is the process of media distribution. This obviously means getting the content to the consumer. It also involves delivering the appropriate licence to use the content according to the offering the end user has selected. Transaction capture is also part of this process: what content has been used by which end user. This information is of course essential for accounting accurately both to the content providers and the service providers.

The third part of the structure is the content management element. This involves the receipt and storage of the media from the content provider. It also involves storing the rules set by the content provider for the exploitation of the content in way that ensures the content is only available as the content provider intends – through particular service providers and in particular territories.[18]

Most of the technology used to support these processes has been developed internally by OD2; the rights management functionality is, however, provided by Microsoft through its Windows Media technology. This can involve the use of the Windows Media Encoder for converting the original content into the compressed digital audio format that will be used in making the content available on line; the Windows Media Rights Manager for encrypting the content in the compressed digital format; the Windows Media Manager, technology used by the aggregator in the issuing of licences for the content and for transaction capture. Finally the DRM component of the Windows Media Player is the technology on the end user's PC which implements the rules granting permission for certain acts to be performed by the user in relation to the content.[19]

[18]For further information see www.ondemanddistribution.com/eng/home/home.asp

[19]For further information see www.microsoft.com/windows/windowsmedia/drm.aspx

This is a very compressed and simplified description of a highly complex set of technologies and operations but it suffices to show how the different roles and functions are structured within a system that brings content on a protected basis to a consumer. It should also be understood that there are many other ways for making content available to users on a protected basis, some of which have been used successfully for many years. The most common of these systems is what has been termed "secure vending" where content is available from a secure source but once legitimately acquired by a user, the content is able to be freely circulated by that user in unprotected form.

The Microsoft DRM system and others like it are distinguished by two essential features. The first of these is the ability to deliver the rules for the use of the content independently of the content; the second is that the content is persistently protected even when acquired by a user and can only be accessed and used according to the permissions granted to that user. In this way, content downloaded for use on a particular device cannot be transferred to a second device unless the permission obtained by the user for that content expressly permits such a transfer. Looking further into the future, it is possible that charges for use of content on a pay per use basis might be varied according to the age of the material. Current systems implement much simpler business models –subscription arrangements are the most common – due in part to the complexities examined elsewhere in this report. This should not obscure the fact that certain DRM systems can and will be used for implementing much more complex rules, particularly in the business to business environment, in the near future.

One of the models that has been under consideration for many years is what is known as superdistribution. This involves effectively inserting DRM into the peer-to-peer mechanisms, enabling consumers to freely share content files through file sharing networks but only in a way that ensures that the usage occurs on terms established by the content provider.

Whatever the complexities and the current state of systems it is safe to say that the use of DRM enabled systems is in its infancy and that significant developments can be expected in the coming months and years.

Conclusion: Although a considerable number of DRM enabled solutions are available in the marketplace, their limitations have to be recognised. None of the available solutions cater for all content types and platforms and there remain major issues of interoperability and access. If content services are to provide a significant push to the take up of broadband there must be a concerted effort by industry and government to create the optimal conditions for the development of DRM enabled solutions and their adoption by the widest possible range of content providers. This effort must also focus on minimising the costs and risks that content providers are faced with in bringing their services online.

Issues

The changing commercial environment

Traditionally there has been little integration of value chains and distribution channels for different types of content: recorded music, publications, computer games and videos have flowed to the consumer from the producers via wholesale and retail operations more or less independently. This has been changing at the retail level in the past few years as product lines of different content types have been combined to produce the range of goods required to inhabit large retail spaces. (A content mega store typically requires at least 100,000 product items – music, videos, books and periodicals, computer games - to be viable).

Digital convergence is reinforcing this trend as consumers prefer one stop shopping experiences when looking for content for a variety of digital applications. Online retailers such as Amazon are taking this process still further, essentially making it the norm in developed markets for the retailing of traditional content carriers – CDs, DVDs, computer games etc.

As the internet began to come into its own as an environment in which to conduct business so the notion of "disintermediation" grew in popularity. The thought was that content providers would be able to deal direct with their customers and dispense with the intermediaries in the value chain. Now, with the dotcom era behind it, industry is realising that commerce structures and value chains on the internet, while involving some new players, are not so radically different after all (as can be seen from Fig.1 in the preceding section). What does change, of course, is the commercial dynamic of the value chain in terms of margins, cash flow and customer relationships.

What also changes is that from at least the retail point in the value chain (e.g. the ISP) and possibly from the content aggregation point (as in Fig 1) one sees an accumulation of different content types, all feeding into the same end user services.

It is important to note in this context that there is a need at each point in the value chain to insert new rules or conditions[20] with regard to the use of the content. For DRM tools and systems to support a multi-layered commercial value chain they need to allow for the definition and delivery of rules and conditions independently of the encrypted content. They also need to be configurable in order to support a rule setting hierarchy.

The issues which the content provider has to address in this environment are an inevitable downward pressure on content values through the integration of different content channels and the relative margins, particular those of the service providers, involved in bringing the content to consumers.

Conclusion: The information society, while not changing the fundamentals of the value chain, has introduced new elements into existing value chains and created new value chains with industry sectors which have previously never interacted. The negotiation of revenue splits and commercial arrangements between these new partners are a major challenge for industry.

---

[20]Such as the price or duration of a deal (licence)

Metadata, rights data dictionaries and rights expression languages

It follows from the nature of the DRM enabled transaction process described in the preceding section that machine readable language is required to express the relevant intentions of the providers and users of the content. Whilst such machine readable languages may provide the syntax to express these requirements they do not deal with the semantics, that is, the meaning of terms used in the messages. This may appear trivial when the communication is simple but becomes infinitely more difficult when there is a requirement to express complex concepts to significant numbers of parties. There is therefore a need for the development of rights data dictionaries that enable the conveyance of commonly understood meaning within the rights expression language messages. The rights expression languages are therefore the grammar of Internet communications, whilst the rights data dictionaries provide the dictionary definitions of each term.
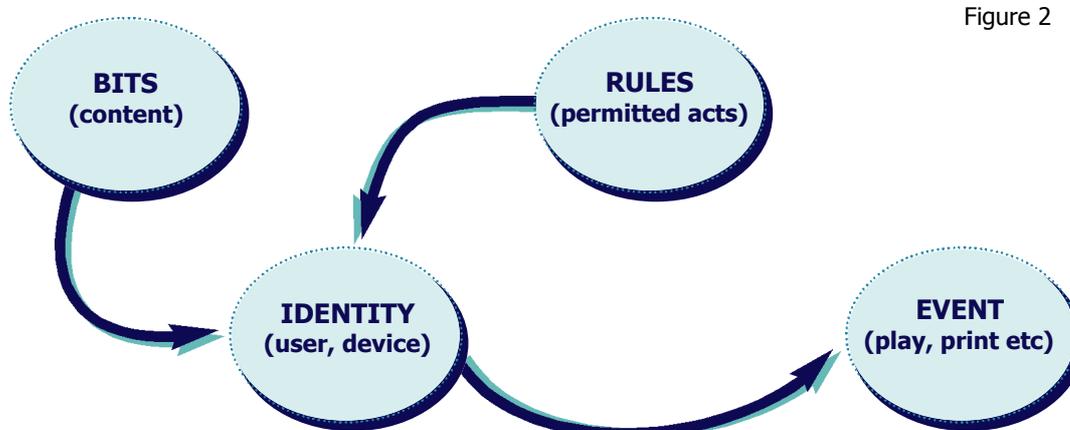
Figure 2

BITS
(content)

RULES
(permitted acts)

IDENTITY
(user, device)

EVENT
(play, print etc)

The four elements in figure 2 are the elements of a DRM transaction. Content (bits) is made available by one party to another with an authenticated identity for access and use according to particular rules. Once the content, the identity of the user and the rules are in alignment, the transaction is given effect: an event occurs i.e. an instruction is executed within the device to, say, print a document. The identification and expression of the different components is necessary for the functioning, security and accounting of the transaction. This is in addition to the identification of parties and content required to facilitate their location and to support usage of systems generally.

Breaking this down into specific propositions, content requires identifier systems; persons and devices may need identifying beyond their native identification (e.g. John Smith or the serial number of the device); rules need to be expressed in a form which is intelligible to both humans and devices.

Many forms of content already have identifiers developed for them as objects of intellectual property: ISBN (publications), ISRC (sound recordings), ISWC (musical works) and ISAN (audio-visual works) are all examples of content for which identification or metadata (i.e. data about data) has already been developed. Another example, although with much broader application potential is the Digital Object Identifier system. Many other identifier standards could be cited. The important question about all of these systems is their adaptability to the digital management of content – and the reference here is to the importance of integration mentioned in the introduction – and their compatibility within different user platforms: interoperability.

The rights data dictionary and rights expression language requirements lie at the heart of any effective, DRM enabled, on-line content system. It is obviously a broad and complex requirement and again, the issue of interoperability is fundamental: different platforms – PCs, PDAs, mobile phones and MP3 players – should all be able to read and apply the permissions attached to particular content.

From a usage point of view, the task of the rights data dictionary and the rights expression language in respect of content embodying intellectual property rights is an interesting one. Traditionally, of course, the rights in such content have been established by statute. This statute – copyright law – reserves to the holder of those rights the choice whether to authorise third parties, in relation to the content, to perform acts falling within the scope of those rights. In the absence of that permission, such acts are unauthorised and proscribed by the statute. And where permission is granted it is usually carefully worked out both in scope and terms.

In the DRM enabled environment those traditional forms of expression have to be converted into forms which will adequately instruct the computing device to perform the act which is the object of the permission. This is a complex task for any form of rights data dictionary and rights expression language to accomplish for a number of reasons.

First, the terms taken from a rights data dictionary and communicated using a rights expression language, unlike the statutory derived rights expression, function by reference to the object of the permission. The rights granted under copyright law are expressed by reference to acts, expressed in fairly generalised form, which are restricted to the owner of the rights. It is the licences granted in respect of such rights in relation to particular acts and particular content that provides the additional definition but even this is always subject to some degree of interpretation. The use of terms from a rights data dictionary communicated using a rights expression language functions somewhat differently in that its object is to specify precisely the act (or event) which is authorised to occur pursuant to particular instructions. The function of these two technologies may therefore be better expressed as managing "permissions" rather than "rights".

Secondly, the very precision in the functioning of a machine and the way it reads instructions to obtain meaning as to the permissions being expressed involves other complexities. Heavy reliance is placed in traditional forms of rights expression on the context in which the permission is implemented and/ or in which the content exists. When a consumer purchases a book in a shop, she is not confronted with the precise scope of the permission granted in relation to the intellectual property in the book. Indeed, while contracting for the purchase of the book with the shop, she has no nexus by way of express licence with the intellectual property right holder at all. The range of acts she is permitted to perform in relation to the contents of the book have to be largely assumed, implied or imposed by the nature of the medium. There are many acts however which may in fact be restricted in relation to contents of the book: she is not allowed to create a copy for sale; to quote from the contents excessively and certainly not without attribution; she is not allowed to publish a translation of the contents; she cannot make a film of the contents. The list goes on but since most consumers would have neither the means nor the inclination to perform many such acts, the restrictions can be safely left implied. Within those limits the consumer is pretty much free to do what she wants with the contents, only falling foul of the actual restrictions when her acts threaten the normal commercial exploitation of the contents.

Not so, of course, with digital content management where no act is possible in relation to governed content without express permission. The "fuzziness" of traditional rights expression and usage is lost and it soon becomes clear how important that generally accepted margin of fuzziness becomes to the normal exploitation of content.

Can the combination of rights data dictionaries and rights expression languages find some way to embody in useable form this contextual element?[21]

A third and related complexity is that of imbuing the combination of rights data dictionaries and rights expression language with sufficient richness to perform all the functions that are possible using traditional forms of rights expressions. The Publishers' Association is, for example, focusing considerable attention on whether the emerging technologies are adequate for their needs, particularly in licensing the rights in publications at the wholesale level. It is one thing to develop tools to express permissions to end users within a value chain; it is a somewhat different and certainly more complex process to develop technologies which express those terms which are pertinent to the relationships higher up the value chain.

In an important sense perhaps, these complexities, once recognised are beneficial in seeking to establish if not a single, at least a limited number of standards in the area. Producing the kind of standard required here is a massive undertaking and it is unlikely that many different initiatives will be able to deliver a sufficiently comprehensive and workable standard.

Against this background, there follows a review of the major initiatives in the field. The objective of the OASIS[22] Rights Languages Technical Committee provides a useful starting point:

"Define the industry standard for a rights language that supports a wide range of business models and has an architecture that provides the flexibility to address the needs of diverse communities that have recognised the need for a rights language. The language needs to be:

- Comprehensive: Capable of expressing simple and complex rights

- Generic: Capable of describing rights for any type of digital content or service

- Precise: Communicates precise meaning to all components of the system

- Interoperable: Comprehends it is part of an integrated system

- Agnostic: To platform, media type of format

- Use XrML[23] as the basis in defining the industry standard rights language in order to maximise continuity with ongoing standards efforts.

- Define a governance and language extension development process that maintains and evolves the language while minimising the negative impact of change on all stakeholders."

---

[21]See David Weinberger, Copy Protection Is a Crime (Wired, US Edition, June 2003)

[22]Organisation for the Advancement of Structured Information Standards: www.oasis-open.org; OASIS is a not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. OASIS produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps and interoperability within and between marketplaces. OASIS has more than 600 corporate and individual members in 100 countries around the world. OASIS and the United Nations jointly sponsor ebXML, a global framework for e-business data exchange. OASIS operates XML.org, a community clearinghouse for XML application schemas, vocabularies and related documents. OASIS hosts The Cover Pages, an online reference collection for interoperable markup language standards. The OASIS Network includes UDDI, CGM Open, LegalXML and PKI.

[23]XrML is a general purpose language in XML used to describe the rights and conditions for using digital resources. It also provides mechanisms to ensure messaging integrity and entity authentication with XrML documents. Specification available from: www.xrml.org

The principal initiative in this area is that of MPEG 21. The rights data dictionary and rights expression language components of the MPEG 21 multimedia framework are intended to comply fully with the OASIS criteria listed above.

Other REL systems exist: ODRL was independently developed in Australia and has attracted some interest, particularly from the Open Mobile Alliance (OMA) which is working to create open standards for the mobile telecommunications platform.

The development of interoperable rights data dictionaries and rights expression languages able to function in relation to diverse forms of content across different platforms is essential to advanced digital content services. At the same time the effort to develop them should be driven by the need to find analogues for the rich permission granting structure developed over many years in traditional (i.e. statute and contract based) systems of rights management. While there may be a justification for "keeping things simple" at this stage with a view to kick starting the market where these technologies will be used, the future need for more sophisticated solutions must be kept in mind. The importance of MPEG 21 is very clear in this context but even here it would be desirable to clearly resolve any uncertainty regarding the application of its rights data dictionary and rights expression language to the adequate expression of contractual terms at wholesale or distribution points in the value chain.

Recommendation: The UK content industries should jointly commission a study into the application of the emerging rights data dictionaries and rights expression languages to the licensing and management of copyright materials. Particular attention should be paid to the relationship with traditional systems of rights administration and whether the emerging languages are adequate for dealing with complex rights transactions at the wholesale level - the area of "contract expression languages". Consideration should also be given to the use of rights expression languages in public sector applications of DRM tools and systems and whether these give rise to any particular needs in addition to those already identified by the private sector.

Timeline: Before the end of 2003

Recommendation: Government should actively promote the development and promulgation of global DRM-related standards. The standards including those of metadata, rights data dictionaries and rights expression languages should be established by the private sector through existing international standards bodies, such as ISO. Government should also actively engage with the European Commission to ensure that the latter adopts a similarly pro-active agenda for the development of global standards.

Time Line: Ongoing

E-payment and billing systems

This is a vitally important subject and is included for a number of reasons. First, since getting paid is a primary consideration for commercial online content activities and some public sector services the subject is fundamental to enabling online content services. Secondly, the current inadequacies of the options available to content providers and their business partners have to be highlighted. Thirdly, with such a limited number of options, their impact on a host of commercial and consumer issues is of major significance. These include the choice of business models; the definition of markets, both demographically and territorially; the flow of consumer data; and the service/consumer relationship generally.

It is easy to assume that given the existence of credit and debit cards, utility (especially telecommunications) payment aggregation and billing systems and sophisticated payment systems established for digital television services, accessing an appropriate system for the online purchase of content would be relatively straightforward. This is not the case. The hope was as the age of the internet dawned that there would soon become available a number of efficient electronic micropayment systems. Unfortunately, one by one bold ideas and major players have fallen by the wayside including those such as Digicash and Mondex.

The reasons for these failures are not hard to find and do not lie for the most part in any shortcoming in the technology used. They are rooted in the enormous complexity of creating an interoperable, cost effective and secure global infrastructure for the movement and processing of monetary value. The issues are immense and ones that it has taken the world's major financial institutions many years to master be they risk related, cost related or structural.

Closed payment aggregation and billing systems do offer various possibilities in terms of the business models that can be used to support this but they have other limitations which reduce their overall usability. In terms of options that are interoperable and have global reach, the only option is the major global credit card systems – and again they come with important limitations.

Credit cards

There is a common assumption that payments for online content services can be effected through credit cards because that is how most online purchases are done. The assumption is somewhat flawed however because it overlooks the important restraints on their use in certain markets and in respect of certain business models. Consider first the extent to which credit and debit cards are used in different markets and by different demographics.

Spending on cards as a proportion of GDP 2001 (%)

	Debit	Credit	Total
UK	9.96	10.32	20.28
France	11.0	0.42	11.50
Germany	4.27	0.16	4.42
Italy	3.05	0.32	3.37
Spain	3.77	3.29	7.06

Source: CCRG

A further demographic limitation is found in the general absence of credit card availability in the youth market, the principal market sector for certain content providers – the music industry and to some extent the games industry.

Credit card transactions involve minimum transaction fees because of the risks and processing costs taken on in respect of each transaction by the issuing banks and the credit card companies. These are highly developed structures but the global acceptability and protection they provide to their customers obviously come at a significant cost. As a consequence, while systems are well established for efficient online purchasing with credit cards they cannot be used for the kind of micro payments that would be used in a pay per use business model for certain kinds of content: again, music is an obvious example. In these instances the content providers are left with no option but to go with models that the credit card system will support such as subscription services or online analogues of traditional models: outright sale of content.

Whatever the limitations, credit cards remain for the time being by far the most common payment and billing system used. This has other consequences. Credit cards also provide a basis for defining the territorial location of the user and thus the rights that are available to that user. This may; however, conflict with the actual location of the user and the content and rights that based on actual location would ordinarily be available to that user. The subscriber to a service such as Emusic who uses a US issued credit card to pay for the subscription to the service will be able to access content according to the US rights deal regardless of where in the world the user may access content from. In time this situation could lead to significant distortion in the international rights market.

Existing billing systems

Alternatives to the credit card systems are available but as pointed out above come with their own particular restrictions. It is quite possible that existing payment aggregation and billing systems established or operated by internet, cable, digital TV or telecommunications service providers may be developed to support digital content services. However, given these are closed systems, it does mean that a consumer might need to establish multiple accounts for different platforms and types of content and content providers would be denied some economies of scale in the processing of revenues.

Electronic wallet

A third option is the use of an electronic wallet where for example electronic credit is established for a consumer using a credit card and which is decremented each time a piece of content is used by that consumer. Such a system could accommodate micropayments and thus a greater variety of business models but at least some of the credit card restrictions remain, at least in the background. Furthermore, at least two other significant problems complicate the scenario: consumer attitudes to prepaid budgets and the security issues of administering such a system particularly one involving the local storage of credit. Prepaid telephone cards and the popularity of, for example, the Belgian Proton cash card suggest that the first of these issues is not a major obstacle. The second, the significant security issues, would certainly seem to be. Interoperability of different wallet systems and across different platforms is also difficult to achieve.

Customer ownership

The consumers for particular kinds of content could reject prepaid budgets. The alternative credit budgets may well require the involvement of institutions - such as banks, credit card companies, telecommunication and other utility type entities – with established customer relationships involving detailed credit histories. The credit payment relationship might well create a basis for these intermediaries to end up "owning the customer", possibly to the detriment of the content or service provider. In addition, where DRM enabled pay for play business models involving the collection of usage data are used, similar considerations with regard to access to and ownership of that customer usage data – commercially, extremely valuable information - generated through the system will become a major issue amongst the various participants in the value chain. These issues are complicated further by particular demographic considerations such as the establishment of credit relationships with the youth market and the personal data requirements associated with that relationship.

The whole area of payment and billing systems is highly complex. As their use becomes more pervasive they could bring profound changes to the established economic order within which content providers and the other participants in digital content value chains have traditionally operated. When content providers and their distributors consider the various options a host of questions have to be answered. These would include:

- Who controls the payment and/ or billing system?

- What are the system costs to the content provider and the value chain participants?

- How will value flow to the different rights holders and value chain participants?

- How is control exercised and what safeguards (system safeguards, in addition to regulatory safeguards) are in place to prevent abuse of dominant positions?

- How will these systems be regulated?

Conclusion: The lack of ubiquitous e-payment systems remains a significant barrier to the enabling of digital content commerce. The current solutions do not cater adequately for micro-payments necessary for many new business models, in certain consumer sectors and for the interoperability demanded by consumers across platforms.

Recommendation: Government should commission an in-depth study into the area of electronic payment and billing systems. It should ascertain the scope of application of existing systems, find out what content providers need from e-payment systems and assess the prospects for development of existing and new systems to meet the demands of the various consumer sectors, markets and business models.

Time Line: Complete by end of 2003

Legal issues

The international copyright standards contained in the WIPO treaties which emerged in the second half of the 1990s[24], along with regional[25] and national laws[26] implementing those standards embody the proposition that copyright law has a key role to play in relation to the DRM. In particular, specific provision was made for penalising interference with – "circumvention" - of technologies applied to the protection or management of rights. A second area of copyright law impacting on the use of DRM is the maintenance of certain exceptions and limitations to copyright in certain circumstances. These are in general well-established both as international standards and as features of national law including those relating to libraries, archives and educational institutions. Others such as the private copying exception have emerged in national laws on an ad hoc basis as a fix to challenges to basic copyright principles from so-called disruptive technologies.

The BSG DRM Group has not conducted an in-depth review of the relationship between the application of copyright law and the use of DRM tools and systems for subject matter covered by copyright. It has however noted the growing number of complexities surrounding this relationship. These include the difficulties of reconciling, in the implementation of the EU Copyright Directive, the regulation of technical protection measures and existing systems implementing exceptions to copyright protection.

They also include the controversies that have arisen in connection with the anti-circumvention provisions of the US Copyright Act. Worthy of mention in this connection are two cases:

U.S. v. Elcomsoft   (formerly U.S. v. Sklyarov)

The case involved Advanced eBook Processor (AEBPR) software developed by Dmitry Sklyarov, in Russia, for his Russian employer Elcomsoft. According to the company's website, the software permitted eBook owners to translate from Adobe's secure eBook format into the more common Portable Document Format (PDF). The company maintained that the software only works on legitimately purchased eBooks. Dmitry Sklyarov was arrested when he came to the United States to give a talk on computer security and the case has proceeded from there. Eventually charges against Sklyarov under the DMCA for violation of its anti-circumvention provisions were dropped and instituted instead against his employer, Elcomsoft. On 17th December 2002, Elcomsoft was found not guilty. The case brought an outcry of protest from a number of civil rights organisations.[27]

---

[24]WIPO Copyright Treaty; WIPO Performances and Phonograms Treaty; Geneva, December 1996. See also the WIPO publication: Intellectual Property on the Internet: A Survey of Issues. December 2002 available at: http://ecommerce.wipo.int/survey/html

[25]EU Copyright Directive: Directive 2001/29/EC

[26]The Digital Millennium Copyright Act of 1998; see: www.loc.gov/copyright/legislation/dmca.pdf

[27]See www.eff.org for further information

Lexmark v. Static Control Components

On 30th December 2002 Lexmark, the maker of computer printers, filed a complaint against Static Control Components Inc. alleging the latter had infringed it copyrights in software it used to ensure that only Lexmark ink cartridges could be used in its printers. It also claimed that a violation of the DMCA had occurred through the defendant's circumvention of the secure "electronic handshake" mechanism between the Lexmark printers and that company's ink cartridges. The District Court in Lexington, Kentucky found for Lexmark on both complaints and granted an injunction against Static Control Components preventing the sale of its competing ink cartridges. Static Control Components has subsequently filed a petition with the US Copyright Office to exempt them from the anti-circumvention provisions of the DMCA technology that "(does) not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance."[28]

These cases raise an important point. As stated elsewhere in this report the use of DRM tools and systems for the protection of content is governed by principles relevant to all forms of content, whether or not such content is of a kind traditionally protected by copyright law. Accordingly while providing remedies for interference with technical measures is obviously essential, the standard for such remedies should be considered against the general scope of the use of such technical measures. In short, the Group questions whether the nature of the content protected by DRM should be the sole determining factor in setting the level of sanctions for interfering with the DRM technology. Whether or not the facts in the Sklyarov case justified the actions taken by the US Department of Justice or whether the use by Lexmark of technology to secure a market advantage was consistent with competition considerations, the fact remains that the basis for both cases was the interference with security measures.

The issue of ensuring that DRM tools and systems are not applied to create an advantage for content providers not sanctioned by intellectual property laws is an important one but unlikely to prove as critical in practice as some commentators would suggest. Many areas of uncontrolled use of content whether sanctioned by law or not will continue regardless. Other uses of content – private copying, for example – will no doubt, in the fullness of time, be resolved through developments in technology and business models.

An area of particular interest is the application of DRM tools and systems for creating content usage rules where exceptions and limitations to copyright have been developed in the public interest. This would include for example the use of copyright materials in education and libraries where, as is discussed in more detail elsewhere, the environment may be highly conducive to the establishment of particular DRM enabled rule sets. DRM should not be seen as an obstacle to these public interest exceptions and limitations but rather as the vehicle to assist in their efficient implementation.

It is tempting to advocate a wholesale revision of copyright based on the greater understanding of technology as applied to content and rights that is already emerging but that is very unlikely to happen. Having said that the DRM Group believes it is essential for regulators in the sector to have much greater regard to the impact of technology.

---

[28]See a note on this case by Chris Sprigman at http://writ.findlaw.com/commentary/20030325_sprigman.html

Conclusion: The debate about exceptions and limitations to copyright continues to rage. Some protagonists see the use of DRM as an aggravating factor which disturbs the balance at the heart of copyright in favour of rights holders. While recognising the complexities of the issues the DRM Group prefers to explore the potential of DRM to provide new solutions in the area. It is, for example, quite possible for a number of public policy exceptions and limitations to be implemented within closed networks, e.g. libraries, schools using the rule setting and enforcement capabilities of DRM. The role of DRM tools and systems becomes even more important as these closed systems become increasingly internet based and merge into the publicly accessible environment. Legislators should take note that, while DRM, in conjunction with other measures, has the potential to manage well-codified copyright exceptions, there is a cost attached to these solutions and it is likely that those costs will rise the broader and more complex the exceptions become.

Recommendation: The content industries and public sector beneficiaries of copyright exceptions (such as libraries and education) should work together to create frameworks for use of content, employing DRM systems to enforce the agreed scope and terms of use. Government should facilitate definition of the complex issues related with this proposition.

Time Line: Ongoing

Consumer issues

It is important to consider in detail the impact of the new technology on consumers because their confidence in systems will determine the take up not only of particular services but also the viability of the underlying service infrastructure. Obvious issues include the following:

It will be argued that giving up certain kinds of personal data – such as personal content usage history - is the price consumers will have to pay to enjoy new business models such as pay for play. But is there to be effective regulation of that price and by whom? Who effectively "owns" personal data; can it be traded between content providers and other value chain participants in total disregard of the interests of the data subject? Should the data subject enjoy some residual or inalienable rights in respect of personal data? What are the necessary but at the same time commercially workable safeguards required to protect the identity and personal data of minors – a critical demographic sector for many content providers. Are there commercially viable reasons for developing and deploying ways for consumers to use digital content management technologies for protecting their personal data? While many of the data protection issues have, in principle, been determined by the European Data Protection Directive, DRM may assist companies in meeting the operational implications of these requirements.

How effective is the growing body of e-commerce legislation around the world, and particularly in Europe, in balancing the interests of content and service providers with those of consumers? What criteria should be met in order to promote an orderly development of new services without alienating consumers?

What protection can a consumer be guaranteed against the loss of digital content and/or associated usage rights against mechanical failure; against unjustified revocation of rights by service or content providers; against the loss of content or rights through arbitrary formats or system changes by service or content providers? How does a consumer return digital content? What dispute resolution mechanisms are available?

The Copyright (Visually Impaired Persons Act), which came into force in 2002, provides for the copying of materials on behalf of visually impaired users. This copying usually means changing the format of the original to one which is accessible using adaptive or assistive technologies. However, changing the format in this way is generally interpreted as an act of unauthorised use by DRM systems. There is a clear tension between the statutory rights of the disabled person and the need to deploy real-world DRM solutions. It is essential that this copyright exception is enabled in DRM solutions to preserve the right of access, just as it is in the design of online services. The Guide to the implementation of the Disability Discrimination Act Part 3, which comes into force in 2004, makes specific reference to a requirement that web services must be accessible. Organisations must make reasonable adjustments to their digital services to ensure that they are accessible. The Disability Rights Commission is surveying 1000 UK websites during the Autumn of 2003 to check compliance with the Act.

How should consumer protection be regulated and enforced in a way which is understandable to both content providers and consumers? Should it be exclusively mandated by legislation or implemented and enhanced by codes of practice? What is the possibility of creating international (as opposed to regional) standards? The answers to these and other questions will have a very real impact on the willingness of consumers to subscribe to the new systems.

Recommendation: The content industries should take the lead in addressing relevant consumer confidence-building measures through establishing codes of practice. Within the bounds of competition regulation, areas to be covered by these codes could include data protection; technical support and back up services; licence revocation; service and product guarantees; charge back and return mechanisms; alternative dispute resolution.

Time Line: By Spring 2004

DRM in the public sector

The BSG DRM Group does not consider there to be any essential distinction between the private and public sector in their use of DRM tools and systems for the management of digital content. The application of security technology to digital content management is an all embracing proposition.

The take-up of broadband in the public sector both for internal administration and for interfacing with the public will be a critical factor in achieving the government's overall broadband objectives. At the same time, the deployment of standardised DRM tools and systems can bring real advantages to the public sector including data protection; the reduction of overhead costs; the reduction of paperwork; the improvement of workflow efficiencies; optimalisation of workforce productivity; reduction in the costs of workforce training. Government is, of course, a major customer for broadband as well as a major content provider.

Information security is critical in many areas of public life and administration. The scope for applying DRM-enabled systems is therefore substantial and might well be relevant to many of the following areas:

Government and local administration
- procurement
- financial management
- peer to peer working
- tax collection

Education
- national curriculum on line
- higher and further education
- inter- authority curriculum sharing
- new learning media and tools
- shared learning over broadband
- digital content online

Health and social services
- administration of medical records
- medical teaching over broadband
- diagnostics and remedies over broadband
- distance health care

Home and defence
- immigration services
- criminal justice administration

Museums, archives and libraries
- preservation and cataloguing of resources
- lending
- commercialisation of resources
- digital content online

In some respects the public sector provides a much more conducive environment to develop understanding of how DRM tools and systems can work in practice. For a start the ground is already well prepared with, for example the eGIF[29] standardisation protocol and the Athens[30] authentication system. The tasks for particular applications of DRM are already well defined both in terms of administration processes and public interface needs. Above all there is greater commonality in requirements and standards typical of a more homogeneous environment. It should also be stressed that government is a major producer of content as well as a major customer for broadband services.

A further advantage of developing the use of DRM tools and systems in the public sector would be to provide working proof of the proposition that these tools and systems are agnostic as to their field of deployment and can be used for the management of digital content and the rules which govern its use in any environment. This probably provides the key to resolving the current controversies about "digital lock up" and the interaction generally between the use of DRM and the established exceptions and limitations to copyright protection: rules derived can be written to accommodate the exceptions and limitations to copyright which have been established for public interest reasons.

Recommendation: The Government should implement a small number of pilot public service broadband offerings, deploying DRM applications and e-payment systems.

Time Line: At least three pilot schemes to be operational by summer 2004

---

[29]www.e-gif.org. The e-Gif provides the standards for joined up government and for information to flow seamlessly across the public sector to provide citizens and businesses with better access to government services. In addition, by adopting pragmatic and widely used Internet and World Wide Web standards, the framework aligns government with the trend within industry and serves as a basis for reducing the costs and risks associated with carrying out major ICT projects.

[30]www.athensams.net; An Access Management System for controlling access to web-based subscription services. Athens is, fundamentally, a central repository of organisations, usernames and passwords with associated rights. It has extensive account management facilities for organisations to create and manage usernames and passwords, and to allocate rights to individual usernames. Each organisation who registers with Athens has an Athens Site Administrator, whose responsibility it is to manage these accounts, and ensure that only current members of their organisation have the rights of the organisation. It is also the responsibility of the Site Administrator to ensure compliance with all appropriate licence conditions. Athens also offers organisations the opportunity to devolve or federate authentication to their local authentication service such an LDAP Directory Service, or Kerberos.

The international context

In Europe, three Directorates General of the European Commission have initiatives running in relation to DRM. DG Enterprise has commissioned a study of DRM from the standardisation agency, CEN/ISSS. The report was published for public comment in February 2003[31]. The report contains a useful compendium of current systems but does not [currently contain] any synthesis of the different views expressed by the contributing industries regarding the definitions, requirements and features of DRM. On the other hand, it is debatable how far the original terms of reference were implemented particularly the following:

> "…to further identify all significant effects, including those effects relating to market or technology issues that currently and potentially accelerate or hinder the implementation of DRM in the marketplace."

That said, the BSG DRM Group has expressed the hope that this report can be kept current and thus serve as a useful reference work generally on DRM.

DG Information Society published what it calls a "Commission Staff Working Paper" on DRM in February 2002[32]. Since then it has held a number of Workshops with different affected sectors; a concluding session was held in March 2003 to review the findings of each of the preceding workshops. The outcome was inconclusive and information regarding the Directorate's future plans has yet to be made public. In an associated process, DG Internal Market is considering DRM in the context of copyright and collective management of rights.

In the US, the Technology Administration at the US Department of Commerce has been studying demand side issues impacting broadband roll-out and adoption.[33] Its investigations included the holding of two roundtables on the question of Digital Content and Rights Management[34]. Its final report listed a number of actions for government and business to undertake:

- (For national government)
  Protecting intellectual property and supporting digital content
  As market players work to develop technologies, standards and business models that enable digital content and rights management, governments can take several steps to strengthen the intellectual property rights framework. By prosecuting clear violations of law, educating citizens and students to respect IPR in the digital medium, protecting consumers' interests (such as fair use rights), and encouraging market players to cooperate and coordinate, the federal government hopes to increase the pace with which movies and music venture online.

---

[31]www.cenorm.be/isss/DRM/draft_report1_2.pdf

[32]Digital Rights Management: Background, systems, assessment. SEC (2002) 197;
http://europa.eu.int/information_society/topics/multi/digital_rights/doc/workshop2002/drm_workingdoc.pdf

[33]Office of Technology Policy, US Department of Commerce, Understanding Broadband Demand: A Review of Critical Issues; Washington; September 2002

[34]See transcript of proceedings of the roundtable on July 17 2002 at
http://205.156.22.252/reports/TechPolicy/DRM-020717.htm

- (For innovators and entrepreneurs)

Developing DRM solutions
Finding technical solutions to copyright challenges will expand digital content willing to go online, especially entertainment, and increase the value proposition for subscribers.

Improving e-commerce quality of service
(security, authentication & micropayments)
Broadband demand will grow as we attack and solve many of the issues hindering quality of service in e-commerce – guaranteeing data rates, authenticating users quickly and securely, paying for goods and services without delay or burdensome forms, and transmitting reliable voice over IP over public networks, for example.

There are a number of political and legislative initiatives underway in the in the US. Proposed legislation from Senate Commerce Chairman Fritz Hollings to mandate the use of DRM technology in IT and CE products has lapsed and is unlikely to be revived. Congresswoman Zoe Lofgren (D-San Jose – the heart of Silicon Valley) has recently re-introduced legislation[35] to provide consumers with certain protections against what she sees as the digital lock up threat from DRM. Legislative proposals along similar lines were also previously introduced by Congressman Rick Boucher[36].

As noted above, the US Digital Millennium Copyright Act and in particular S. 1201 dealing with anti-circumvention of rights protection and management systems is coming under increasing attack from civil rights organisations, consumer groups and the scientific (cryptographic) research community. It remains to be seen whether these efforts will coalesce into any significant effort towards legislative reform. The Register of Copyrights who is empowered to review the provisions every three years – somewhat in the same manner as is proposed for the Secretary of State in the Patent Office's consultation proposal for UK implementation of the EU Copyright directive – has shown little inclination to do more to date than address marginal issues.

South Korea has the most advanced broadband market in the world, and 9.2 million - over 60 percent - of its households now have broadband. While government action has been important in this development – a nationwide optical fibre network was put in place by 2000 – the real reason for these developments is seen in the coming together of content services and demand from consumers at grass roots level[37]. Gaming culture in Korea is strong and it is estimated that 75 per cent of broadband users consume audio and video content over their connections; for example they pay a small fee to watch a TV show they missed earlier in the day on their TVs. PC gaming has been a strong driver for broadband uptake, with the old and young taking an already-established game-playing obsession online. NCsoft is now the world's largest online gaming company with about two million users paying around £15 per month for services.

[35]See: www.house.gov/lofgren/congress/lofgrenbalance2003.pdf

[36]See: www.house.gov/boucher/docs/dmcrahandout.htm

[37]See: A Comparative Study of Broadband in Asia: deployment and Policy; Izumi Aizu; Tokyo; September 2002

The most popular method of payment in Korea is through pre-paid accounts by way of mobile phones. These account for 48.8 per cent of transactions by value. The other systems are ARS, similar to the above but using landlines, at 24 per cent by value, credit card payment (20 per cent) and having charges added to monthly ADSL bills.

There are a number of companies developing DRM tools and systems. The best known of these is Fasoo[38], a division of Samsung. Although Fasoo is now concentrating on enterprise DRM applications it was associated for a number of years with InterTrust Technologies and worked to develop DRM solutions for consumer content such as music and e-books. Other companies include Sealtronic[39] and Digicaps[40].

Recommendation: The BSG should conduct an international review of the impact of online content services on the take-up and use of broadband. Particular emphasis should be placed on studying rights management and payment systems used in the delivery of these services.

Time Line: Complete by end of 2003

---

[38]www.fasoo.com

[39]www.sealtronic.com

[40]www.digicaps.co.kr

The bottom line

Neither the potential nor the limitations of DRM are widely understood at present. Content industry executives need to be able to envisage commercial strategies in which DRM tools and systems play a central part not only as value chain regulators but as a means for helping to define the commercial offering; copyright lawyers should see DRM as more than a mechanism for implementing copyrights and which in turn depends on copyright laws for its protection. Technologists need a better understanding of the complexities of law, commerce and social interaction, important parts of which function beyond the reach of code, be it legal or computer. Every effort must be made to develop a common understanding.

Recommendation: The BSG should bring together the various stakeholders in the digital value chain to explore new business models.

Time Line: First initiative to be held in September 2003

Government, too, has to pay more attention to DRM and its related issues. A search of a number of UK government websites – DTI, DCMS, UK Business Online – under both "DRM" and "digital rights management" came up with a single, marginal reference.

If the UK is to take the lead in the provision of online content services, helping in turn to drive take-up of broadband, then there has to be a concerted effort between government and industry to provide the necessary information and educational resources for both content providers and users to acquire the knowledge they need to make online content services a "must have" proposition. DRM is a crucial part of that knowledge base. This report therefore concludes with perhaps, at least for the immediate future, its most important recommendation:

Recommendation: Industry and government should work together to bring relevant information about DRM and related elements of the online content service infrastructure to content and service providers, to their customers, to government and other public institutions.

Time Line: Work should begin by September 2003 with first products to be available by January 2004

In so recommending, the BSG DRM Group hopes that the contents of this report constitute a useful first step in that process.

Acknowledgement

About the Broadband Stakeholder Group (www.broadbanduk.org)
The Broadband Stakeholder Group (BSG) was established by Patricia Hewitt in April 2001 to advise the government on the development and implementation of a strategy to enable the UK to meet the Government's target to have the most extensive and competitive broadband market in the G7 by 2005.

Since then the BSG has continued to act as the single focal point for all stakeholders to address both short and long-term issues related to the deployment and take-up of broadband services. Several working groups were established and are continuing to pursue ongoing work programmes.

The BSG has continued to build effective relationships with key private and public sector stakeholders, including the DTI and the Office of the e-Envoy and a number of key governmental departments and related industry bodies such as the OGC, Digital Television Stakeholder Group and the Information Age Partnership. Secretariat support is provided by Intellect, partly funded by the DTI.

Broadband Stakeholder Group
20 Red Lion Street
London WC1R 4QN
T +44 (0)20 7395 6731
F +44 (0)20 7404 4119

Further reading

Bill Rosenblatt, Digital Rights Management (John Wiley & Sons, 2001)

Bill Rosenblatt, DRM Watch: www.drmwatch.com

Gordon E Lyon, A Quick reference List of DRM Standards & Organisations
(NIST, October 2002)

Bruce Schneier, Secrets & Lies (John Wiley & Sons, 2000)

Ross Anderson, Security Engineering (John Wiley & Sons, 2001)

C. Christensen, The Innovator's Dilemma

Simon Singh, The Code Book: The Secret History of Codes and Code-breaking