This article first appeared in the November 2007 issue of PLC Magazine.
©Legal & Commercial Publishing Limited 2007. Subscriptions +44 (0)20 7202 1200

Few can argue that the much-vaunted digital age is now upon us. For those in the digital content business, the exploitation of copyright-protected works by means of digital media presents both great opportunities and great risks. The opportunities to distribute and make digital content available to a global marketplace are opportunities for greatly increased customer bases and revenue streams. The relative ease of producing perfect copies of digital content reduces (and in some cases removes) manufacturing and distribution costs, thereby giving greater opportunities for profit margins for both licensors and licensees of digital content. However, the risks loom equally large.

With global distribution systems, territorial restrictions are difficult if not impossible to enforce. Anyone with a computer and a modicum of knowledge is able to make perfect copies of digital content very cheaply. The impact of these risks has perhaps been most markedly demonstrated in the music industry where sales of UK singles between 1993 and 2003 fell by 43.7 million units or 54.6%. At least some of this fall must be attributable to the fact that current estimates indicate that approximately 7.4 million users have illegally downloaded music in the UK alone.

This article:
• Briefly outlines the legal rights underpinning digital content.
• Looks at licensing digital content and the key terms that such licences may contain.

In the third in a series of articles on rights in digital content, Rachel Boothroyd of K&L Gates outlines some of the key issues that arise when licensing digital content.

Licensing digital content
Opportunities and risks

Illustration: Getty Images
### Drafting digital licences: terms to consider

<table>
<thead>
<tr>
<th>Term</th>
<th>Licensor</th>
<th>Licensee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition precedent</strong></td>
<td>◆ Is the licensee required to obtain third party rights clearance?</td>
<td>◆ Is the licensor required to obtain third party rights clearance in the content?</td>
</tr>
<tr>
<td></td>
<td>◆ Beware of broad representations of ownership of all rights in content (particularly audio-visual content which may contain many layers of rights).</td>
<td></td>
</tr>
<tr>
<td><strong>What is being licensed?</strong></td>
<td>Ensure the licence grant is limited to those rights owned by the licensor.</td>
<td>◆ Consider all rights which may exist in the content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Consider potential for ownership issues in different territories (particularly relevant for online exploitation which may be accessible worldwide).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◆ Seek warranties and indemnities from the licensor regarding licensed content ownership.</td>
</tr>
<tr>
<td><strong>Scope of the permitted acts licensed</strong></td>
<td>Closed, limited list of permitted acts. Consider:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ Defining permitted acts under relevant legislation.</td>
<td>◆ Beware in particular any limitation to reception by device as convergence is rendering devices interchangeable by users.</td>
</tr>
<tr>
<td></td>
<td>◆ Specifying the permitted technical activity.</td>
<td>◆ Seek to “future proof” where possible by reference to technology which is “whether now known or invented after the date of this Agreement”.</td>
</tr>
<tr>
<td></td>
<td>◆ Specifying the permitted delivery and storage media.</td>
<td>◆ Where the licensor seeks to create an exclusive list of permitted media consider insertion of the words “including but not limited to” to increase options.</td>
</tr>
<tr>
<td></td>
<td>◆ Imposing device limitations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ Imposing timing restrictions.</td>
<td></td>
</tr>
<tr>
<td><strong>Exclusivity</strong></td>
<td>◆ Is the licence to be exclusive, sole or non-exclusive? Exclusive rights grants often enable negotiation of higher royalty rates. Exclusivity may be granted for separate permitted acts, for example, an exclusive grant for online rights and also an exclusive grant for exploitation via mobile devices.</td>
<td>◆ Balance exclusivity against higher royalty rates and potentially more restrictive scope of grant.</td>
</tr>
<tr>
<td></td>
<td>◆ If the licensor is granting exclusive rights across different technologies, ensure that the scope of rights drafting is very tight and that there is no potential dilution of the rights by those granted to another “exclusive” licensee due to technology convergence.</td>
<td>◆ If the licensor is granting exclusive rights across different technologies, ensure that the scope of rights drafting is very tight and that there is no potential dilution of the rights by those granted to another “exclusive” licensee due to technology convergence.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td>◆ Will often wish to limit the term.</td>
<td>◆ Often the longer the better.</td>
</tr>
<tr>
<td></td>
<td>◆ May be a balancing act between term and royalty rate.</td>
<td>◆ Balance with risk of technology convergence or changing consumer habits diluting the exclusivity or value of the rights negotiated.</td>
</tr>
<tr>
<td></td>
<td>◆ May be advantageous to link royalties generated by the licensee to options to renew the term.</td>
<td></td>
</tr>
<tr>
<td><strong>Territory</strong></td>
<td>◆ Only license and potentially warrant/indemnify use in the territories in which you own rights. This is a particular risk when online rights are granted and the parties may be considered to be aware that online use may be accessed worldwide.</td>
<td>◆ Worldwide is frequently best and reduces enforcement difficulties (for example, problematic online territorial restrictions).</td>
</tr>
<tr>
<td></td>
<td>◆ Link to an obligation on the licensee to deploy technology to limit access from unlicensed territories.</td>
<td>◆ If worldwide nature is the reason for the licensor resisting the grant of warranties/indemnities, this could potentially be split to give the warranties and indemnities only for the territory in which the licensor feels able to do so, but to retain the broader grant of rights.</td>
</tr>
<tr>
<td><strong>Warranties and indemnities</strong></td>
<td>◆ Seek to limit as much as possible.</td>
<td>◆ Warranties and indemnities particularly desirable with regard to potential third party rights infringement for online use but these may be difficult to obtain.</td>
</tr>
<tr>
<td></td>
<td>◆ General contractual/licence considerations to prevail.</td>
<td>◆ General contractual/licence considerations to prevail.</td>
</tr>
<tr>
<td><strong>Assignment and sub-licensing</strong></td>
<td>◆ For many digital licences to distributors, consideration will need to be given to the terms on which the distributor may make such content available to end users. For maximum control and risk management, set out the terms of an end user licence agreement in a schedule or specify some of the critical terms to be included in the end user licence agreement.</td>
<td>◆ Important to consider what is required on a practical level to enable end users to use content as anticipated.</td>
</tr>
<tr>
<td></td>
<td>◆ Alternatively, specify what acts will be permitted by the end users. This may be supplemented by obligations to implement digital rights management (DRM) technology to prevent end users from doing anything else.</td>
<td>◆ Consider whether you will be able to enforce any restrictions imposed on end users (again, DRM considerations are important).</td>
</tr>
<tr>
<td>Term</td>
<td>Licensor</td>
<td>Licensee</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Assignment           | ● Is the identity of the licensee important in the decision to grant this licence? If so, include restrictive assignment provisions. In any event, it is prudent to only assign with the licensor's consent.  
● For the same reason, consider including change of control provisions. | ● Might you want to re-sell the licensed rights via an assignment? If so, include the right to assign (even if this is with the licensor's consent).  
● If the content is to become a key asset of your business, and the business may be acquired or sold, the right to assign again is important. Also, beware of any restrictive change of control provisions. |
| Digital rights management | ● Include an obligation on the licensee to use "effective" DRM.  
● Licensee may resist taking liability for the consequences of any failure of DRM. An alternative would be to either approve the DRM that will be used by the licensee or an obligation to use the most up-to-date DRM to restrict non-licensed uses. | ● Avoid taking liability for the consequences of failure of DRM; with the current state of technology this will almost certainly lead to liability. This would include any obligation to use "effective DRM" as arguably any breach of DRM via hacking or otherwise would render the DRM deployed as non-effective.  
● An obligation to deploy DRM is very likely to be included and one method to limit liability may be to agree the protocol with the licensor.  
● Alternatively, the licensor may subscribe to one protocol for DRM technology across all of its content licensing in which case it may specify exactly what is required. |
| Royalties | The options are almost limitless but include:  
● A minimum royalty for an initial period after which you may want to terminate.  
● Tie royalty/payment to the licensee's revenue generation streams.  
● Digital content uses have shown high potential for high revenue generation from new or unforeseen services. Methods to review the actual revenue received by the licensee and tying the royalty or other payments for the content use to benefits to the licensee are worth considering.  
● The direct content licensing revenue stream may not present the whole story on licensee value. Much of the benefit to a licensee may not be from sale of the content itself but for tied hardware sales advertising. | Again, the options are varied.  
● There may be a benefit to limiting royalties to a percentage of direct purchase of content by end users as value may be derived from the content through other sources, such as hardware purchase or advertising or subscriber revenues.  
● It is important to be very clear when describing revenue streams attributable to the content to ensure that, if this is not intended, other indirect revenue streams are not included. |
| Termination | In addition to the usual boilerplate terms:  
● Consider immediate termination rights if there is a risk of third party infringement or if DRM is breached.  
● Immediate termination rights may be required due to the potential for rapid and perfect digital copies to be made of circulated content. | ● Resist termination for "suspicion/risk" of third party infringement as this allows significant discretion to the licensor to terminate. A right for the licensor to suspend only in these circumstances or appointing an independent expert may be the compromise on this.  
● Consider damages for termination by the licensor where it turns out that the licensor's concern was not well founded. |
| Post-termination | ● Take particular care with obligations to remove stored materials. The licensee may have stored the content on back-up systems or it may be cached. Expressly referring to any long-term or intermediate storage of content is helpful in the obligations post-termination. | ● Although the licence may terminate, a distributor of content may still have obligations to end users or the end user licences may be perpetual. Important to ensure that termination of the head licence does not create a breach of any such obligation. |
| Licence back | ● Useful information may be generated, together with adaptations of licensed content, such as user data. A licence back of any such material is worth considering.  
● Data analysis (neutralised to remove any data protection issues) may be very useful to the licensor to indicate uses or methods of exploitation of the licensed content. | ● Data or new content created through a licensee's exploitation of licensed materials may have its own intrinsic value. In particular, tracking data and statistics of usage has been found to be valuable. If requested by the licensor, and if it is not a problem for the business to make available to the licensor, this information can be used to reduce the price or otherwise gain benefits in negotiation. |
| Personal data | ● Although a licensor often wants access to the customer names for the licensee, this is not automatically permitted under data protection law.  
● If access to customer names at the end of the licensed term or even during the licensed term is important to the licensor, the licence should include specific provisions compelling the licensee to include specified opt-in/opt-out questions for the users, as this will give the highest chance of being able to transfer the data in compliance with data protection legislation. | ● Beware of a request from the licensor for customer data as, unless certain conditions are met, you are unlikely to be able to transfer such data legitimately without taking specific measures to enable this.  
● If a licensee would prefer not to provide this data, data protection legislation may often be cited as a shield to any such request. |
• Examines the role of digital rights management (DRM) in the enforcement of licence terms and underlying intellectual property rights.

UNDERLYING RIGHTS
Before drafting or negotiating a licence of digital content, the parties must examine the underlying rights in the digital content to be licensed, how these apply to digital content and the potential ambiguities (for background, see feature article “Rights in digital content: an overview”, www.practicallaw.com/6-374-2029).

Copyright
Under the Copyrights, Designs and Patents Act 1988 (CDPA), as amended by the Copyright and Related Rights Regulations 2003 (SI 2003/2498), a copyright owner may prevent others from carrying out the following key acts in relation to content and so may seek to commercialise these rights via the grant of a licence:

• Copying of a substantial part (section 17, CDPA). Copying may be intangible (for example, by appearance on a website) or tangible (such as the production of a photocopy). Even if a copy is not visible to the eye, bear in mind that copying may take place. Most licences of digital content will need to grant the right to produce copies.

• Issuing copies to the public (section 18, CDPA). It is currently a subject of debate as to whether this includes online as well as offline distribution. There is an argument that publication online on a website is only the issue of one copy (and so there is arguably no breach of section 18 of the CDPA unless the plural is construed so as to include the singular), as opposed to the issue of multiple copies as would be required for offline distribution. This may, for example, be relevant to caching (see Glossary) activity by a search engine.

• Renting or lending copies to the public (section 18A, CDPA). It is more likely that this applies to both online and offline distribution, as it is more widely accepted that the plural includes the singular.

• Performing, showing or playing in public (section 19, CDPA). It is critical to determine whether any performance does in fact take place or whether it is in fact just a communication of a performance, which would be covered by “communication to the public” (see below). So, for example, the public display of a digital screen on which a dramatic performance is streamed may fall within section 19 of the CDPA. The act of streaming itself is covered by the communication to the public offence.

• Communication to the public (section 20, CDPA). This covers the traditional broadcast right and the new right of “making available to the public”. This “making available” right is key for licensing digital rights and essentially relates to any “on demand” service. The important factor is that the work is “accessible from a place and at a time individually chosen by [the user]”. This could be e-mail distribution, pay-per-view services, peer-to-peer transmissions or even a repeated broadcast at regular intervals of the same programme.

• Making an adaptation of the work or doing any of the above acts in relation to an adaptation of the work (section 21, CDPA). The right to adapt is important for digital content, as it is often an essential right for licensees where there may be format issues for reproduction of the content on different devices, such as mobile phone screens (see box “Devices for receiving digital content”). Licensor should always consider whether a licence back of the adapted content is required or desirable. They should also consider whether they require an advance approval right for adapted content. For example, re-configuring picture size can lead to picture distortion, so if image integrity is important licensors may want to monitor adaptations using approval rights.

Devices for receiving digital content
Digital content can currently be received on a range of digital devices, such as:

• Digital television.
• Digital recorder systems (TiVo, Sky+).
• Digital radio.
• Desktop/laptop PC.
• Mobile device.
• Special devices for receiving digital content:
  • e-book (Sony reader, Copybook).
  • Tablet PC (HP/Compaq TC1000, Nokia 770).
  • Video game console (PSP, Nintendo DS).
  • Digital music player (iPod, Zen, Zune).
  • Personal digital assistants (Blackberry, iPhone, Treo).

Despite an apparent mismatch between the copyright legislation wording and the rights to be granted in a bespoke licence when defining the licensed activity, it is important to include the copyright-specific language. The grant clause can then be further refined by adding appropriate technical details (see “Key licence terms” below).

Database rights
For digital content, database rights arguably extend their reach way beyond tables of data and what we would normally consider as databases. For example, there is an ongoing argument as to whether a web page constitutes a database (NVM v De Telegraaf, CA The Hague, 21 December 2000; Algemeen Dagblad a.o. v Eureka, President District Court of Rotterdam, 22 August 2000). It appears to satisfy the key elements of the definition, being a collect-
tion of independent works, data or other materials which are arranged in a systematic or methodical way and which are individually accessible by electronic or other means (section 3A, CDPA).

A web page is also likely to pass the “sufficient investment” test required for database protection (section 13(1), Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)). To cater for this possibility, a digital licence grant should therefore permit a licensee to “extract or re-utilise” any database contents (for background, see feature article “Database right: a narrower scope of protection”, www.practicallaw.com/6-201-2791).

Trade marks and image rights
These are often embedded in, and intrinsic to, digital content. As such it is important to be alert to this fact when preparing bespoke digital licences and to include a grant of trade mark rights and any so-called image rights where required, particularly when dealing in theatrical licences in countries which have specific image rights or personality rights protection.

KEY LICENCE TERMS
Licensing is at the core of the marketplace for digital content. It is the legal means by which the content owners can leverage the value of their assets and the content-hungry digital platforms and networks can acquire the necessary content to drive traffic, revenues and market consumption.

Licensing is of course not a novel legal structure, but the subject matter is new and developing almost daily. Digital licensing does not fit easily within the established legal framework, despite attempts such as the introduction of the Directive on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (EC/2001/29) (see News brief “UK copyright law: adapting to the information society”, www.practicallaw.com/7-102-5119) and the imminent Audio-Visual Media Services Directive, and there are many difficulties in matching the commercial possibilities presented by rapidly advancing technology with established legal definitions and structures. When drafting a digital licence, there are many issues to be considered (see box “Drafting digital licences: terms to consider”), including the following:

Use
One of the first questions to ask when drafting a bespoke digital licence is “a licence to do what?” For digital licensing, this is often not easy to answer. It is essential to understand the types of technical use that a bespoke licence is expected to cover. This applies to both the licensor and the licensee. Generally, the licensor will want to restrict the licence to a narrow grant of rights, while the licensee will want to ensure it has as broad a grant as possible. When drafting a grant of rights, each of the following technical areas should be considered:

- The technical activity. This may overlap with the underlying rights such as “copy” but is likely to be much more sophisticated. Examples include cache, host, stream, zip and download.
- Delivery and reception. Careful thought should be given to the definition in the licence of the media to be used for delivering and storing the content, for example, internet transmission (bearing in mind the distinction between the web and the internet), VPN transmission, DVB-H, DAB, closed network IPTV or free-to-air TV.

Equally important will be provisions limiting the reception of digital content to specific devices such as a mobile handheld device or a computer (see box “Devices for receiving digital content”). Device restrictions are tricky to pin down due to the rapid convergence of technologies. For example, what is a television in today’s society? Is it possible to watch digital television on a computer screen, so does this make a computer a television? Licensees in particular need to be cautious with device restrictions, although in practical terms it may in fact be impossible for a licensor to enforce a licensee restriction permitting it to only transmit content for reception on “television”.

Timing restrictions
These apply to live events such as sports events and concerts. There is significant value in live rights but also in other permutations of timing for digital transmission. Different licensed categories of rights include “live”, “near-live”, “non-live” and “delayed”. High value sports rights are packaged and valued on the basis of timing divisions such as these.

Future-proofing
Any digital licensor should be thinking about how to guard against technological advancement when technology is de-
veloping at such a rate. There are many licences in existence which were drafted before the internet was even thought of but which grant online rights as the licences contain broad grants of rights with no reference to platforms or devices (for example, a grant of “audio-visual rights”) and without any reservation clauses. As a result, some licensors have lost potentially significant revenue streams. A licensor of rights under any bespoke digital licence today should include provisions to guard against such unwitting grant of rights for use on future-developed technologies. Equally, a licensee must ensure that the scope of granted rights is sufficiently broad to ensure it captures developments in the technology on which the licensee intends to distribute the content.

This is not a new risk created solely by the digital revolution. In 1919, the age of silent films, a licence granted Walt Disney the sole and exclusive rights to produce Peter Pan in “cinematograph and motion picture films”. The Court of Appeal confirmed (obiter) that this language would be sufficiently broad to grant rights to both silent and the new technology of “talkie” films (Hospital for Sick Children v Walt Disney Productions Inc [1968] Ch 52).

Any licensor wishing to “future-proof” a grant of rights should include the following two key provisions:

• Unless rights are specifically granted, they are reserved and belong to the licensor.

• Technology not invented at the time of the grant is not covered by the licence.

Equally, a licensee will be concerned to ensure that its rights are protected in the event of the introduction of a new technology which is substitutional or complimentary to the granted technology (see box “Future-proofing”).

DIGITAL RIGHTS MANAGEMENT

Licence terms alone do not sufficiently influence consumer behaviour with digital content to manage the risks presented by digital copying, and DRM has developed as a technical means by which licence terms may be enforced. The “holy grail” of DRM is to impose technical restrictions on what may be done with content in order to ensure that copyright owners maintain control of their work and receive compensation for their investment. Given the ease with which unprotected digital content can be copied and distributed, it is often argued that DRM protection is essential to prevent the collapse of the traditional sales-based revenue model for the exploitation of digital content. Although copyright is protected in the UK and the EU, and so in theory each person who makes an illegal copy of a CD, carries out an illegal file download or shares a digital document without authority may be subject to legal action, the scale of the problem of illegal copying in the digital age often makes it impracticable to locate and bring claims against the individuals involved.

Legal definition

The All Party Parliamentary Internet Group defines DRM as “the generic term for a set of technologies for the identification and protection of intellectual property in digital form” (Digital Rights Management - Report of Inquiry by the All Party Internet Group). In legal terms, DRM is split into two components:

• Technological prevention measures (TPM) which are “any technology, device or component which is designed, in the normal course of its operation, to protect a copyright work other than a computer program” (section 296ZF(1), CDPA).

• Rights management information (RMI) which is “any information provided by the copyright owner or the holder of any right under copyright which identifies the work, the
author, the copyright owner or the holder of any intellectual property rights, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information" (section 296ZG(7)(b), CDPA).

RMI is the expression of the rights of the owner, licensor or licensee and how the work can be used (for example, the work may be listened to but not copied, or downloaded once but not forwarded). Accordingly, RMI may be simply the expression of the licence terms. TPM is the technology which ensures that the rights are enforced. It is an offence to circumvent the DRM applied to any digital content and/or to manufacture, market and sell devices which carry out such circumvention (sections 296, 296ZA and 296ZB, CDPA).

Problem areas
There is not yet a universally accepted DRM protocol. Licensors will often seek to impose stringent DRM obligations on licensees. Equally, licensees may demand DRM encoded content to enable them to protect the licensed content or enforce their licence terms. When deciding what level of DRM burden to include in a licence of digital content, and with whom this burden should sit, issues to consider include the following:

- There is an argument that DRM interferes with standard property rights and often imposes restrictions on the use of content which are stricter than those for previous media, such as video tapes or CDs. For example, anyone can purchase a book, CD, DVD and then give or sell it to a third party. Most DRM software will prevent a buyer from legally purchasing digital content and then passing or selling it on to someone else.

- In general, copyright will expire in a work at the death of the creator plus 70 years. In contrast, DRM restrictions (if effective) are permanent, in essence granting a permanent copyright.

- DRM does not recognise the individual user and so does not recognise “fair dealing” exemptions (see box “Fair dealing exemptions”). For example, it often prevents the disabled from accessing digital content because the specialist software used to convert the content to Braille or speech does not work with the DRM software. This could lead to possible challenges for discrimination under the Disability Discrimination Act 1995 for companies using DRM.

- The technology may become outdated leaving the purchaser of the

---

**Glossary**

**Caching.** Storing copies of web pages which have already been downloaded in the hard disk of a personal computer, avoiding the need to repeatedly download each time a user wishes to view the content and therefore speeding up web access.

**DAB (digital audio broadcasting).** A technology for broadcasting audio content using digital radio transmission.

**DMB (digital multi-media broadcasting).** A digital transmission system for sending audio-visual broadcast signals to mobile devices. This system competes with DVB-H.

**Download.** The retrieval and transfer of data from a remote computer using the internet (or other network), the retrieval of data to a computer’s random access memory ram or the retrieval of data for storage on a hard disk.

**DVB-H (digital video broadcasting – hand held).** A technical specification for transmission of audio-visual broadcast services to handheld devices. This system competes with DMB.

**Host.** To store and manage pages of text, images or other information on the web or a local area network (LAN) and provide any associated scripts, databases and software so that the pages are accessible to others via the internet or the relevant LAN.

**Internet.** The global communications system of computer networks accessible by the public which interconnect, either directly or indirectly, individual computers and/or networks and which enables users to engage in two-way transmissions of data over such networks in order to transmit and receive content.

**Internet protocol.** A network layer protocol used for communicating data across a packet-switched network.

**IPTV (internet protocol TV).** A system enabling digital television to be delivered using internet protocol over a network infrastructure.

**Streaming.** The transmission and/or receipt of a sound or video file at the same speed or quicker than regular play speed. In this way users may watch an audiovisual “clip” as it downloads.

**VPN (virtual private network).** A communications network operating through the public internet but accessible only to a limited user group as users require explicit security features to access the network.

**Web.** A network of interlinked documents and resources residing on the internet that use hypertext protocols and language, which are available for display using browser software.

**Zip.** Method used to reduce the storage capacity required by a file so making it quicker to send over the internet. Zipped files usually have the file extension “.zip”.

---

This article first appeared in the November 2007 issue of PLC Magazine.
©Legal & Commercial Publishing Limited 2007. Subscriptions +44 (0)20 7202 1200
content without the ability to access the content. This could be a major problem for libraries and other archives which may create archives of digital content.

• Interoperability is one of the biggest problems caused by DRM. The two major DRM technologies are Microsoft Windows Media DRM and Apple Fair-Play. Files in one format are not supported on the other and vice versa. Different download suppliers sell music files with one of the DRM technologies: for example, iTunes (DRM version) uses Apple Fair-Play and this means that non-Apple devices such as the Zune may not be able to play the files and vice versa. The fact that DRM can tie the consumer to a particular device or set of devices presents competition law issues. Complaints have been made to the European Commission about the closed nature of the iPod - iTunes DRM link.

• Other legal issues may be created by seeking to divide markets by use of DRM. For example, Apple is currently under investigation by the European Commission for the way in which it is making use of DRM to prevent downloads from different EU member states. The price of content on iTunes varies by country; for example, a download costs more in the UK than in Germany. It is argued therefore that Apple is using DRM to prevent UK citizens from downloading German content onto a UK iPod contrary to the principles of the single market.

Possible solutions
One option is to remove all DRM. This has taken place to some extent in the music industry but has often led the content provider into conflict with the record labels. Apple announced in April (at the time of the EU investigation) that it would offer DRM-free tracks from EMI. Rather than using DRM, the tracks contain personal information about who and where they were purchased which would, if necessary, allow the copyright holders to track any illegal content back to its original source.

The types of technologies that are able to embed this type of information include:

• Digital fingerprinting. This is used by Apple in its “DRM-free” content and embeds information (such as e-mail address and location of purchase) into each user’s copy of digital content, which can be extracted to help identify culprits when an infringing copy is found.

• Digital watermarking. This adds specific information to the original data content file (called a watermark). The original creator or distributor of the file can look at the watermark of any given file to see if it has changed as a result of copying. It also embeds the identity of the owner of the copyright into the work so that they can be identified in cases of infringement.

The solution adopted by many licensors and licensees of digital content is often a compromise. One party takes the obligation to introduce DRM, and the protocol or technology forming that DRM may be agreed or left to that party’s discretion. Bearing in mind the ongoing European Commission investigations regarding the iPod-iTunes DRM link, it is worth considering including provisions in the licence for the parties to review the effectiveness and viability of any relevant DRM in the event that the use of DRM proves to be contrary to any law or regulation.

Rachel Boothroyd is a partner and head of the intellectual property and technology group at K&L Gates in London. She would like to thank Helen Smith, a senior associate at K&L Gates, for her help with this article.