Chapter XV
Legal Issues for DRM: The Future

Vagelis Papakonstantinou
University of Patras, Greece & PKpartners Law Firm, Greece

ABSTRACT

DRM systems have been implemented in the past few years by the Content Industry as the panacea against all copyright (and Intellectual Property Rights in general) infringements over the Internet. The validity of this statement shall be assessed in this analysis, identifying its strengths and record to-date and highlighting its shortcomings in an increasingly complex e-commerce (Web 2.0) environment. While doing this, particular attention shall be given to (mostly EU) Intellectual Property Law, Consumer Law, Data Protection Law, and Competition Law.

THE (LEGAL) BACKGROUND

Before embarking upon the legal analysis of contemporary DRM e-commerce systems, as elaborated in other chapters of this book, a short presentation of the background that led to their development is deemed essential. DRM systems, as it will immediately be seen, have been the Content Industry's technical, but not necessarily legal, response to a relatively recent and otherwise unprecedented volume of attacks against the copyright scheme, that could have ultimately brought its demise. Nevertheless, DRM e-commerce systems, essentially reflecting business rather than technical models, it remains to be seen whether they will indeed fare well under the legislative environment that regulates a number of their aspects.

The Digitization of Information

The digitization of information signaled the first difficulties for the copyright scheme[1]. Until that time the copyright system for protecting intellectual property had worked relatively successfully for around

200 years. It was first developed in the United Kingdom back in 1709[2], when the development of printing and the sale of legislative (and Shakespearean) texts begun evolving into an industry[3]. Law-makers of the time identified thus a new type of property, "intellectual" property. This had not been as evident then, as it perhaps appears to us today: for thousands of years before that time, property was divided into only two categories, fixed assets (land) and mobile assets (furniture, equipment, garments etc.). Only at that time did mankind realize that works of the intellect could be of an economic value, and therefore constituted "property" of their author (or right-holder). In this sense, the system that was then developed, and is still in use today, focused upon protection of the "work" of the intellect against unauthorized reproductions (copyright = right to copy). The author of such a protected work deserved compensation for each and every use (reproduction, copying) of his work by others.

The digitization of information challenged the practical, not theoretical, parts of this scheme. Until then reproductions (copies) of any "work" were relatively easy to control (and thus, ask for a fee): books had to be printed and sold on bookshelves, music had to be copied into vinyl and sold on record stores, paintings could only be seen at the premises of the person who owned them. All these actions of reproduction included cost (and thus could not be undertaken by anyone), and were controllable because of the relatively small distribution channels (shops) and the fragmented market (international commerce meant totally different things at the time). The digitization of information managed the first blow to this scheme: once texts and music and pictures became digital, anyone could reproduce them at minimum cost. No more were printing and binding machines or vinyl-cutting industries needed; once "works" became digital, anyone, even home users, could easily copy and store them in their computer systems for (unlimited) future use. Evidently, the 17th century scheme, whereby any act of copying would confer money to the author of the work automatically became obsolete: copying became so vast that the Content Industry could no longer control it as effectively as it did in the past. Even when new "works" emerged (for instance, movies) it was only a matter of time before digitization affected them in the same way too.

The Internet (Mostly P2P) Factor

The Internet managed the second, and crucial, blow to the copyright scheme: it increased exponentially the distribution channels. Until its emergence the digitization of information, regardless whether annoying in itself for the content industry, remained inevitably "computer-isolated": any user could store tons of protected material in his computer, but use essentially was confined to his computer alone. Because networks did not exist (at least outside the academic or work environment) any exchange of protected works with other users had to be performed physically, by means of copying onto a disk and carrying the disk to another computer in person. Consequently, even at that time the Content Industry was not particularly discomforted[4]: although its property was digitized and copied massively, user-isolation meant that purchases of originals were not substantially affected.

Once the Internet emerged this was no longer the case: connected users were suddenly able to exchange "files" (incorporating unauthorized copies of copyrighted material) without moving from their homes, at a single press of a button and at a marginal cost. Traditional distribution channels (i.e., shops) were shattered. No longer was it necessary at least for some users to purchase the original in order to digitize the work in it – the, vast, Internet community made sure that once a single user in the whole wide world purchased the original and digitized it everybody could then have it for free through a simple download[5].

To make things worse, e-commerce systems emerged that enthusiastically (probably too enthusiastically if they knew what was good for them) facilitated the exchange of files among users, namely Peer-to-Peer (P2P) networks. This development was probably inevitable, given the user interest in it. E-commerce systems are inevitably innovative ways of transforming user interest into money[6]. They may not be predicted beforehand, because they are inherently innovative, transforming new technology into user trends. This has been as much valid ten years ago, when P2P networks were state-of-the-art as it is today, when IPTV, VOD and Web 2.0 systems (for instance, YouTube) are the talk of the day.

At any event, the Content Industry now had to face new e-commerce systems that demonstrated a new way of exploitation of its works. The first to have been affected was the music industry, obviously because songs took up less storing space (with the help of the .mp3 format) and were thus easier to be exchanged through the bandwidth then available. At the peak of an era that such P2P networks as Napster[7] initiated, millions of users rather than buying whole CDs, they broke them apart separating songs and exchanged them for free among them, while income was realized by the facilitator (P2P network, essentially an e-commerce company) through other ways (mainly advertisement).

The battle between the Content Industry (as represented by its music branch) and new e-commerce players (P2P networks) was fierce and lasted a decade. Although a number of cases were initiated by music labels against P2P networks, the one that finally did make it to the US Supreme Court was the one by Metro-Goldwyn-Mayer against Grokster. The question at hand was whether a P2P networks facilitator could be held indirectly ("secondary") liable for the uses of its software by its users (that is, for the unauthorized exchange of copyrighted material among its users). At first[8] the P2P operators seemed like they could get away with it: courts were confused with the, relatively recent VCR cases where VCR manufacturer Sony was not held responsible for copying of TV shows performed by users using its sets[9], and drew the analogy between this case and P2P networks facilitators. Nevertheless, the US Supreme Court held otherwise[10]: based on quantitative and qualitative criteria (for instance, 90% of content stored on P2P networks is copyrighted material, 100 million users exchanged more than 1 billion files on a monthly basis, plus the fact that P2P operators actually advertised this aspect of their systems) it decided, in short, that P2P networks operators are ultimately liable for the actions of their users, and thus made the continuation of their operation in their then form no more viable.

The, American, verdict on Grokster unavoidably affected the way all countries around the world viewed P2P networks. This happened not only because P2P networks could no longer operate lawfully in the USA, but also because copyright legislation constitutes in practice international law. Indeed, the WIPO and the international legal instruments in effect (TRIPS, Berne Convention etc.) have established more or less the same legal scheme internationally. Therefore, although the case on Grokster in not typically enforceable in any other country other than the USA whose Supreme Court issued it, any judge in any other country of the world that will be confronted with it (a task diligently undertaken by lawyers of the music industry[11]) would evidently have to explain extremely well any derogation from its findings. This, in practice, has expectedly put an international lid on all P2P network providers, at least as they were known until then[12].

Emergence of the First DRM Systems for E-Commerce: The iTunes Case

Once the Content Industry had won its battle against the first generation of e-commerce newcomers (namely, P2P networks providers) and it became clear that its content (songs, texts, pictures, and, given bandwidth, films[13]) could not be distributed over the Internet for free, the second generation of e-com-

merce contestants assessed the situation. After Grokster what was known to everyone in the on-line market was that, first, a tremendous users' interest and know-how existed in the on-line provision of content, and that, second, the Content Industry would not be deprived of its lawful interest to compensation for every use of its content, regardless whether on-line or off-line.

DRM technologies for e-commerce applications emerged as the natural response to the above gap: having a strong market of millions of users on the one hand (who, after the P2P demise, where left "homeless"), and, on the other, an industry that was unwilling to provide its merchandise unless assured that its rights would not be compromised, inevitably led to a technology that would gap this gap[14]. DRM e-commerce systems promised to do exactly that: to secure lawful provision (or, to be exact, provision that is according to the preferences of the Content Industry) of content to users.

The legal considerations behind such DRM e-commerce systems will be discussed in the following chapter. Here it is enough to be noted that DRM e-commerce systems ultimately appeal not only to the Content Industry, for self-evident reasons, but to users as well[15]. Users ought not be perceived as systematic law-breakers. Despite of any doubts anyone may cast upon the copyright (and patent) scheme today, the fact remains that users are aware of law-breaking when downloading content online without paying anything for it. On the other hand, the on-line provision of content undoubtedly has its merits: content is available to take with everywhere, to save in various means for reproduction, to process in play lists, and, ultimately, it constitutes, allegedly, a far more enjoyable option that typical CD or DVD purchasing or cinema viewing. DRM e-commerce systems address concerns of those law-abiding users who see no reason why they should be deprived of the merits of the on-line provision of content. By providing a lawful alternative, DRM systems helped the on-line market mature.

An economic model thus had to be devised. DRM e-commerce systems constitute essentially technical solutions – they do not guarantee in themselves any financial success (any more than they guarantee their own lawfulness, as it will later be seen). At any event, the first comprehensive solution that, combined with the appropriate hardware, had tremendous success in the market and today constitutes the "standard" is undoubtedly Apple's iTunes[16].

The iTunes on-line store is a case study in itself that will be revisited many times during this analysis[17]; being the leader in the market, it has attracted international attention not only on its approach (using DRM technologies for the on-line provision of content) but also on some of its finer features (almost exclusive connection to Apple's hardware -iPod, uniform charges for songs regardless of their age or popularity, fragmented, country-specific provision of content etc.)[18].

An analysis of the iTunes model is here only performed for consistency's purposes; readers are indeed encouraged to visit and purchase at least some content, and also try to store it into Apple-connected (iPod) and non-Apple (other mp3 players) means, in order to acquire a first-hand experience of the standard-setting model in the market. At any event, here it is enough to be noted that Apple has setup on-line music stores in several countries of the world; users from each country connect to their respective on-line store, having installed the appropriate software in their computer, and purchase content (mostly music, but also films, TV shows and other items). Content is priced in a uniform way (for instance, each song costs 99p, regardless whether a song of the 60's or the latest hit) and users cannot shop but only in the shop of their country of residence. Once users have purchased a song, it is downloaded in their account. Use of purchased content is far from unlimited: (through use of appropriate DRM technologies) users can, most notably: (a) use their content on "up to five iTunes-authorised devices" (i.e., computers) at any time, (b) store their content "from up to five different accounts on certain devices, such as iPod,

at a time", (c) burn an audio play list up to seven times, (d) are not allowed to burn video content, (e) not allowed to use their content (songs) "as a musical ringer in connection with phone calls"[19].

In the iTunes model we therefore see a DRM e-commerce system in full operation. Its owner (Apple) is using it to restrict use of purchased content. Users buy content (songs, shows, films, audiobooks etc.) at competitive prices, but their rights are effectively limited: they can only use a song they bought in five computers or they can burn it onto a CD only up to seven times. Users are also manipulated into purchasing only from their country's store (thus allowing Apple to gain from exchange rate differences). Appropriate DRM e-commerce systems make sure that these rules are obeyed.

Apple's iTunes is by no means the only DRM model used in the on-line market for the provision of content. Since its first appearance (and success) all possible alternatives have appeared in the market[20]: by now users may pay monthly fees and indeed acquire content without DRM, only streamline content, or pay for any other combination in-between; even Apple (after public criticism, as it will later be seen) has made available, for an additional fee, DRM-free content in its iTunes store. In all these cases DRM systems are the e-commerce providers' such as Apple only weapon, first, to convince the Content Industry to make its products available through their on-line services, and, second, to ensure that rules are observed and their business thus flourishes.

DRM SYSTEMS FOR E-COMMERCE: A LEGAL APPROACH

As already seen, DRM systems for the on-line provision of content have been the e-commerce industry's technical, but not necessarily legal, response to conditions in the market after the Grokster decision. Once it was established that content could no longer be made available on-line without adequate compensation mechanisms for the Content Industry, e-commerce players (most notably, Apple) devised business and technical systems whereby the use of content made available on-line would be controlled according to the standards of the Content Industry who owned it. DRM systems were thus put to this cause.

Of course, DRM systems are by no means newcomers in the field of protecting the interests of the Content Industry. As seen above, off-line DRM systems impeded (and continue to do so) unlimited copying from, for instance, VCRs or DVDs or even CDs[21]. Nevertheless, it was the emergence of e-commerce and the advent of the factors mentioned above (digitization of information, P2P networks) that intensified their use; by now all users over the Internet are familiar with the term and its effect in practice.

It shall therefore be the on-line, e-commerce implementations of DRM systems that shall form the basis of their legal analysis in this chapter. Readers, for practical purposes, may keep in mind while going over this chapter Apple's iTunes; being a leader in the market, its technical implementation and legal approach shall inevitably be repeatedly used as an example.

As regards the particular fields of law that appear to be affected by DRM e-commerce systems, despite of the obvious connection with Intellectual Property (copyright) law, their implementation in contemporary e-commerce practice seems to make several other fields relevant. Most notably, contemporary DRM e-commerce systems find themselves entangled with, at least, Consumer Law, Competition Law and Data Protection Law (Privacy Law) issues. All these fields of law will be elaborated upon in the following paragraphs.

Before embarking upon their examination under a legal point of view a few technical clarifications are deemed essential. Trying to keep the level of analysis as non-technical as possible (technical implementations are elaborated in other parts of this book), within a typical e-commerce DRM system as perceived in this chapter content is expected to follow the so-called *superdistribution* model, whereby "*rules governing its usage are cryptographically attached to the content either directly and or can be dynamically acquired on-line*"[22]. What we therefore have in effect is a system that at its one end attaches cryptographic information onto content, while, at its other end, it sets rules for use of the same content. Evidently, all these actions are undertaken or authorized by the lawful owners (rightholders of the respective economic intellectual property rights) of such content.

DRM e-commerce systems consequently perform two basic tasks: first, they affect "works", in the intellectual property protection sense, by attaching additional information onto them in view of their future use in DRM systems; and, second, they set and implement rules for the further use of such works. It is essentially these two tasks that shall be examined under the said different fields of law in the following analysis.

DRM E-Commerce Systems and Intellectual Property Law

DRM e-commerce systems, as already noted, are the technical, but not necessarily legal, response of the Content Industry to challenges to the intellectual property protection (copyright) scheme. The digitization of information and the emergence of Information and Communication Technologies challenged the viability of a legal framework aimed only at protecting works of the intellect from unauthorized copying. The framework devised in the 17th century withstood all technological and market changes (and the invention of new "works"), based on its strong, factual hold upon acts of copying. When information and communication technologies made copying (private or other) uncontrollable, the whole system crumbled. DRM e-commerce systems aim at re-awarding to rightful owners of "works" control over the use of their property by third parties.

From this point of view DRM e-commerce systems are essentially intellectual property tools. Exactly as with their off-line predecessors (the most recent example pertaining to DVDs), they were created out of a need of the Content Industry, and they purport to properly implement Intellectual Property (copyright) law. It is therefore within this field that the core of the legal analysis pertaining to these systems lies, regardless of the fact that contemporary e-commerce implementations also step into other fields of law such as Consumer Law, Competition Law or Data Protection Law. Such stepping into other fields of law is a by-product of business strategies (for instance, when requesting that content be reproduced only on certain hardware, or that prices are uniform around the world, or that consumers' preferences be recorded) that have ultimately nothing to do with the true nature of DRM e-commerce systems: the protection of intellectual property, within intellectual property law limits, online.

Because Intellectual Property Law constitutes by now more or less international law (thanks to a series of international regulatory instruments, for instance, the WIPO Treaty, the Berne Convention etc.[23]), the approach in this analysis shall essentially focus on the common notions of Intellectual Property Law and not to any, if at all, national particularities. This is deemed necessary, not only because of the, international, nature of Intellectual Property Law itself, but also because DRM e-commerce systems are ultimately e-commerce business models that are addressed to the whole wide world. Being made available over the Internet, their end-users may reside in various parts of the world but, in this context, are subjected to the same, uniform (DRM) rules. For instance, iTunes users acquire the same

rights over content purchased regardless whether they reside within the EU or in America[24]. It is with this in mind that we shall resort to the Intellectual Property Law fundamentals, rather than to, local, particularities.

In the same context, it is evident that when we speak of DRM e-commerce systems and Intellectual Property Law, we speak of copyright. Patents have very little to do with implementing DRM e-commerce systems, at least from an end-user perspective; if any one of those systems infringes existing patents, then this is a totally different issue whose analysis largely exceeds the purposes of this chapter. It is therefore basic copyright legislation that shall form the basis of analysis here.

Intellectual Property Law: A "Safe Harbor" for DRM (E-Commerce) Systems?

Intellectual Property Law is an, ultimately, DRM-friendly field of law; this, however, is done in an indirect way. As far as Intellectual Property Law is concerned, only "*technological measures that restrict acts unauthorized by authors*", the so-called Technical Protection Measures (TPMs), are explicitly acknowledged and protected. In this context, according to the WIPO Copyright Treaty[25], "*contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law*"[26]. TPMs are thus passively protected in the wording above, by means of explicit recognition of their existence in the Treaty. This is, nevertheless, not the only layer of protection afforded to TPMs: in addition to their passive protection, they are also actively protected against (in the case of e-commerce, at least) "hackers": "*contracting parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing [...] that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention: (i) to remove or alter any electronic rights management information without authority; (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority*". Technical Protection Measures (regardless whether in the e-commerce context or other) are thus protected twofold: first, their existence is explicitly acknowledged in the text of law; second, anybody who tempers with them or anybody who passes along content whose TPM have been tempered with, shall be persecuted.

The obvious question now relates to the relationship between TPM and DRM. Despite of the fact that certain views have highlighted their differences (in most of cases with an ultimate aim of justifying attempted circumventions of DRM systems[27]), judging even from their wording their actual relationship becomes clear: TPM are the measures upon which DRM is based. In other words, TPM corresponds to the first of the two basic tasks of DRM systems described above (under 2): the attachment of additional information onto content in view of its later use in DRM systems. And, in the same context, if the act of attaching TPM onto content is recognized and protected by law, most certainly the introduction of (DRM) rules for the use of such (TPM enriched) content is also, indirectly, equally recognized and protected. The use of DRM systems, regardless whether off- or online, is therefore, technically, lawful under Intellectual Property (copyright) Law[28].

Indeed, the e-commerce environment does not seem to affect in any way this statement. In e-commerce models, at least according to the *superdistribution* model seen above, digitised content is affixed with data that shall later be used as instructed by the DRM (e-commerce) system. Evidently, the analysis

above is still valid: TPM is data affixed on works regardless whether they shall be used in the off- or on-line environment. And, DRM e-commerce systems, regardless of technology implemented, essentially use such TPM data in order to regulate users' use of content according to their rules. From this point of view the WIPO Copyright Treaty may be used to accommodate DRM e-commerce systems in exactly the same way it has been used so far to accommodate their, off-line, predecessors.

The same is more or less the situation by now in both sides of the Atlantic. In Europe, the Copyright Directive devotes a whole Chapter (Chapter III) to the "*Protection of Technological Information and Rights-Management Information*". In this context the Directive's Articles 6 and 7 repeat, in effect, the WIPO Treaty's provisions seen above. In the USA, Section 103 of the Digital Millennium Copyright Act (the so-called "*anti-circumvention provisions"*) effectively implemented the same WIPO Treaty provisions. It is therefore safe to say that by now the lawfulness of DRM systems according to Intellectual Property (copyright) Law and as far as its scope is concerned should be taken for granted, both in the off-line and in the online environment.

The DRM E-Commerce Systems Core: The License Agreement

Having established that the first task of DRM e-commerce systems, that is, affixing DRM-related data (in other words, TPM) onto content, is a lawful act performed by rightholders as far as Intellectual Property Law is concerned (and, indeed, Intellectual Property Law is the only field of law that tells us how to deal with "works" or "content"), we now have to establish whether the second DRM e-commerce task is also lawful under the same point of view. In order to do this within an intellectual property context we will inevitably have to look at the terms and conditions of the DRM e-commerce system License Agreement.

It is by now common knowledge that the license to use (but not own) is one of the two ways an author (or, a rightsholder) can make money out of his work. The other way being the transfer of ownership, the license to use shall, for obvious reasons, be the rule in contemporary market conditions. Such "license to use" granted by the rightholder to a user is incorporated into a License Agreement (the all-too-known at least in the Information Technology environment, End-User License Agreement – EULA). However, the particular terms and conditions in a License Agreement are only broadly sketched by (intellectual property) law: apart from a couple of restrictions for the benefit of users (for instance, reverse engineering is allowed regardless what the license says but only for interoperability purposes[29]), an author (or rightsholder) may draw the License Agreement for use of his work by users as he sees fit. It is, after all, under this *laissez-faire* approach that such diverse types of licenses as the standard (commercial) proprietary license (for instance, the MS Windows EULA) and the GPL have been hosted under essentially the same legislative provisions, regardless of their profound differences.

And, it is exactly this possibility for practically endless licensing schemes that makes the task of assessing DRM e-commerce systems' licenses impossible. E-commerce DRM systems do what their owners want them to do. Once it is established, as seen above, that they are allowed to exist, their internal policies and use-specific rules may be as their owners please, provided of course that no mandatory legal provision (and there is only a handful of those in copyright legislation) is infringed. From this point of view, it is simplistic to call DRM (e-commerce or other) systems "good" or "bad"; in themselves, they only constitute tools that (lawfully) regulate use of (copyrighted) works. The use such systems are being put by those who implement them for profit is a totally different issue (and, in most cases, their lawfulness is not for copyright legislation alone to decide).

This is why the License Agreements, the agreements, that is, under which users acquire content, in DRM e-commerce systems should be judged on a case-by-case basis according to Intellectual Property (or other, as seen in the following chapters) legislation. While doing this attention should at first be given to the mandatory provisions of copyright law. Irrevocable rights awarded to users by Intellectual Property legislation cannot be infringed by any contractual terms included in DRM systems' License Agreements. In this context, the European Copyright Directive expressly sets that "*notwithstanding the legal protection provided for [...], in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned*"[30]. What the Directive says, in a perhaps not so straightforward way, is that whenever users benefit from any rights under copyright legislation such rights should continue to be applicable under DRM e-commerce systems as well.

The above been said, it is in fact very few irrevocable rights that are awarded to users by intellectual property legislation that pertain to use of content. Apart from certain categories where special rules may apply (for instance, libraries, education), the rule is that usual, typical users are very much left helpless by copyright law when it comes to DRM systems' policies imposed upon them. Rightholders (the Content Industry) is more or less free to draft the terms and conditions of its (DRM) license agreements as it pleases, at least from a copyright law perspective (other fields of law may not be as accommodating, as it will later be seen).

The only two issues the content industry has to tackle while drafting its DRM license agreements relate to "fair use" in the USA and "private copying" in Europe. According to well-known copyright provisions respectively, in America users are entitled to reproduce works for "fair use" purposes[31]; in Europe, users are entitled to one copy of each work, used for their private purposes[32]. DRM e-commerce systems sometimes (and, it is again reminded that their License Agreements reflect the business models of their owners) get in the way of the above two rights. DRM adversaries have most of the times barricaded themselves behind these two issues. The (legal) analysis of these two cases would largely exceed the limits of this chapter, but would most probably also prove unfruitful[33]. As already seen, it is not in the nature of DRM systems to infringe, for instance, the right to fair use of copyrighted material. DRM e-commerce systems, in their contemporary form (see, for instance, iTunes) only reflect business models, not technological limitations; evidently, if a new law or a court decision set what exactly constitutes "fair use" with regard to current DRM systems implementation, then DRM systems could do nothing but comply; it is therefore to this end that any adversary-DRM resources should be spent. From a *prima facie* approach on typical license agreements of e-commerce DRM systems, it would appear that most of the times they do reflect the existing (regardless how limiting, from the user's perspective) standard copyright provisions.

DRM E-Commerce Systems from the User Perspective

DRM e-commerce systems affect the user perspective, from an Intellectual Property (copyright) Law point of view, in two ways: first, they affect the product he buys. And second, they regulate this, already purchased, product's use in his own hardware. Nevertheless, as it will immediately be seen, the user had better looked elsewhere for effective protection of his rights, than into copyright law.

In the first instance, as already seen, the user, from his own point of view, is interested in purchasing a license to use a specific work, but he ends us with a work that is "DRM-enriched". Whether the user has an option to purchase DRM-without content, or DRM-enriched works is his only way of acquiring them does not constitute an Intellectual Property Law consideration (but rather a Consumer Law or Competition Law question that shall be elaborated in the respective chapters). For the time being it is enough to note that, according to copyright law seen above (under 2.1.1) it is lawful for rightholders to make available media files that do not contain only the work but also other (DRM related) data. From a user point of view therefore, the fact that, rather than buying for instance a license to use a song, he buys a media file containing the song and DRM data, is perfectly fine according to copyright law.

The second task of DRM e-commerce systems is more subtle; they control reproduction of the work, implementing the terms of the respective License Agreement. For instance, a specific song purchased in .mp3 format by a user may not play on all mp3 players, but only on the seller's marketed ones. Again from Intellectual Property (copyright) Law perspective, the user's right to reproduce the work, whose license to use he just acquired, is limited as per the same License's terms. These limitations of reproduction are technically implemented through a DRM system (in the above example, the song just won't load in another mp3 player). Nevertheless, no matter how frustrating this situation may be for the user, the rightholder has in effect all the economic (intellectual property) rights over a work (content), and part of these rights is to grant licenses to use with as many limitations as he wishes (and the market can handle). As long as the rightholder (or, the Content Industry) keeps away from the few (very few indeed, in the case of content) mandatory legal provisions of Intellectual Property Law, the user's right to reproduce the work acquired under a License Agreement may be as limited as (feasibly) possible. DRM e-commerce systems merely reflect this generosity of copyright law to rightholders, but under no means can they be blamed for it by users[34].

DRM E-Commerce Systems from the Author Perspective

Author's rights are probably more relevant when it comes to implementing DRM e-commerce systems under Intellectual Property (copyright) Law. Of course, "authors" in this case do not coincide with rightholders; authors in this chapter shall mean the actual artists who have created the content. As known, when a work is created in the copyright sense, its author automatically acquires economic and moral rights over it; in today's market conditions authors usually transfer their economic rights over their works to the Content Industry (obviously, in return of a fee) and they keep their moral rights (mostly, the right to be recognized as author of the work).

In view of all the above, authors are faced today with some basic questions: first, whether to allow the Content Industry to apply DRM (TPM, actually) data onto their works. Second, whether they do want their works to be made available to users under a DRM e-commerce scheme.

The replies to these answers may not always be straightforward. Although one would expect that the Content Industry, in its contract with the author for transfer of his economic rights, will have provided expressly that the author leaves it at its discretion whether and how to make available the work through DRM e-commerce systems, sometimes this will conflict with the author's inalienable moral rights – and the latter shall prevail. According to the Berne Convention, "*Independently of the author's economic rights, [...]the author shall have the right to [...]object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honour or reputation*"[35]. These rights may not be forfeited under contract.

Authors' therefore do appear to have a choice. The insertion of DRM data onto their works by the Content Industry may be claimed that it worsens the quality of reproduction[36], constituting thus a, forbidden, "*distortion*" or even "*mutilation*" of their work. In the same context, perhaps distribution of a certain work through a DRM e-commerce system that is particularly restrictive and has grown a bad reputation among Internet users may be construed as "*a derogatory action, prejudicial to his honour or reputation*". In all those instances authors do have a right to object against the Content Industry and the DRM systems it implements for distribution of their works. Although here again the lawfulness of distributing works under a DRM e-commerce scheme *per se* may not be challenged by authors (as much as by users), authors have an extra set of rights, their moral rights, from which they could draw if they wished to limit or amend the distribution of their works under DRM e-commerce schemes.

DRM E-Commerce Systems and Consumer Law

As already noted, DRM e-commerce systems essentially constitute "systems" for the on-line use of content: these systems are composed of technical data (TPM, affixed on each "work" in the intellectual property sense) and rules for the use of such (TPM-enriched) content. Once it is established that their existence is basically justified by Intellectual Property (copyright) law, that, as seen above, allows the insertion of DRM-related data onto content, only the rules of these "systems" may be scrutinized under other fields of law. Nevertheless, not all DRM e-commerce systems are run by the same rules; because they ultimately reflect business models of those who implement them, their rules may vary from strict, hardware-limited control over the reproduction of content, to laid back simple cataloguing of users' preferences. This, inevitable, lack of uniformity makes the task of drawing general conclusions on DRM e-commerce systems examined from other fields of law perspective quite impossible. Rather than that, a case by case legal analysis of the rules of each DRM e-commerce systems should be performed each time, in order to assess conformity with other fields of law (that may, after all, be many more than those referred to in this analysis)[37].

This being said, Consumer Law is a field of law that has proven particularly relevant in contemporary DRM e-commerce implementations[38]. Because the Content Industry has often chosen to bind users with strict rules that affect not only the content itself but also the hardware used to reproduce it, more than once Consumer Law, at least in Europe, has come to users' assistance. The analysis in this Chapter shall therefore focus upon these cases, that have formed a first background upon which to judge future DRM e-commerce implementations.

The (Re)quest for Interoperability

Interoperability is seen by many as the "Holy Grail" in the contemporary digital economy. Indeed, after some forty years since the Information and Communications Technologies emergence, the widespread use of computing systems that not always understand each other threatens the foundations of society itself. Our digital economy has come to be based so much in the seamless operation of Information and Communications Technologies that it is unthinkable that any contemporary system will not undertake its best efforts to work in harmony with other (even competitive) systems (evidently, much to the resentment of such systems' owners, who would very much prefer to bind users for ever)[39]. It is after all with this in mind that reverse engineering is allowed by law notwithstanding anything to the contrary in any End User License Agreement:

The authorization of the rightholder shall not be required where reproduction of the code and translation of its form […] are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs […][40].

DRM e-commerce systems ever since their first appearance in the on-line environment flirted with the idea of binding users to specific hardware[41]. Because their owners sometimes also sold their own hardware, the idea of using on-line purchased content to push users towards specific (their own) hardware was understandably tempting; so tempting indeed, that it was put to the test.

It is in this context that iTunes' given preference for the iPod mp3 player should be examined. Apple has implemented in its iTunes Store a DRM system (called FairPlay) that binds together content purchased in it and its iPod reproduction hardware. This has raised considerable criticism on the basis of Consumer Law, at least in Europe. Not only has the EU Commissioner for Consumer Protection asked Apple to change its policy (in her own words, "*Do you find it reasonable that a CD will play in all CD players, but an iTunes song will only play on an iPod? It doesn't to me. Something must change*"[42]), but some Member-States also took action. Most notably in Norway, the Consumer Council filed a complaint with the country's Consumer Ombudsman, accusing Apple of violating the country's Marketing Control Act, and eventually won its case[43]. By early 2007 almost all Member-States (including Germany and France) joined the action against Apple and its iTunes DRM system; by the time this analysis was prepared, however, the negotiations were not concluded.

Sony, nevertheless, has not been as lucky as Apple. Early in 2007 Sony UK and Sony France lost a case against the French Consumer Protection Association UFC Que Choisir, because they did not inform consumers about the lack of interoperability of their mp3 music player with any other content than that purchased from a specific on-line store (Connect). The lack of interoperability worked, in effect, in two ways: Sony's mp3 player did not play any other content than that purchased from the Connect Internet site, and music purchased at the Connect Internet site could be read only by Sony's mp3 players. This tight grip on consumers was too much for French courts, who forced Sony to change it[44].

At the other side of the Atlantic it appears that e-commerce DRM systems have not attracted as much attention as their off-line relatives. Therefore, although Apple's iTunes is prevalent in the American on-line market too, no Norwegian-like claims have been raised so far. On the other hand, Sony BMG's DRM system on its music CDs has attracted so much criticism that it eventually had to settle with the US Government[45].

The above developments clearly set the scene from the Consumer Law perspective. DRM e-commerce systems constitute systems of rules, and it is ultimately these rules that shall be assessed against Consumer Law provisions. The existence of DRM e-commerce systems *per se*, as established by Intellectual property (copyright) Law, may not be challenged by Consumer Law; it is only the rules of these systems that have to be weighted against consumer concerns. In this context, the first years of DRM e-commerce implementation appear to be the probing stage of the Content Industry. Once the on-line model was established (setting-up shops that sell TMP-enriched content aimed at downloading onto computers and/or hardware players) it was worth a try attempting to bind consumers who purchase content on-line to their own hardware, increasing thus their sources of income exponentially. This model, bluntly implemented by Sony and more reservedly by Apple's iTunes, does present the tendency to becoming obsolete. Not only are strict consumer-binding rules clearly not tolerated by, at least EU, Consumer Law, but also the Content Industry itself is trying to detach itself from such image-ruing practices (see, for instance, Apple's sale of DRM-free content, admittedly for an increased price, next

to its other DRM-enriched content). From this point of view consumers seem to have avoided the worst for now; Consumer Law has proven in practice that it is in possession of the filters that will keep the e-commerce DRM model as open (and interoperating) as possible.

DRM E-Commerce Systems and the Protection of Privacy

Contemporary DRM e-commerce systems are expected to gather personal information[46]. Such data may pertain to users' financial information (for instance, credit card details) that will facilitate on-line transactions for the purchase of DRM-enhanced content, users' preferences (simply recorded or actively used to create profiles and suggest further "compatible" sales), users' hardware (if applicable, for interoperability or non-interoperability purposes), users' address (in country-fragmented systems such as iTunes, see below under 2.4.1), etc. This on-line collection and processing of personal information, however, shall invariably fall within the limits of data protection (in Europe) or privacy protection (in the USA) legislation.

Once again it must be made clear before embarking upon any privacy-related analysis that DRM e-commerce systems are perceived as lawfully operating e-commerce systems for the on-line sale of content according to basic Intellectual Property (copyright) legislation. As already established (see above, under 2.1), copyright law justifies all steps necessary for the introduction and operation of a typical DRM e-commerce system. Once this is confirmed, one can only judge this system's rules according to other fields of law: because DRM e-commerce systems essentially reflect the business rules of the business plan of those implementing them, it is only those business rules that shall be assessed against other legislative provisions. And, as far as this Chapter is concerned, typical contemporary DRM e-commerce systems do tend to step into Data Protection (or Privacy Protection, respectively) legislation, through the almost invariable collection and processing of personal information[47].

One further clarification needs to be made before going any further: perceptions of privacy protections vary deeply between both sides of the Atlantic. In Europe (in the EU) a data protection approach has been adopted, whereby formalised rules protect individuals' personal information and state agencies make sure that these rules are observed. In the USA a more *laissez-faire* approach has been adopted, whereby it is individual privacy that is broadly protected (that is, not particularly the processing of personal information) mostly by means of sector-specific legislation; in addition, no federal or state agency is established to centrally monitor the protection of individual privacy. At any event, for the purposes of this analysis, first, "data protection" and "privacy" shall be used as synonyms, and, second, a typical contemporary DRM e-commerce system (along the lines of iTunes) shall form the reference standard.

Collection and Processing of Personal Information

Typical DRM e-commerce systems place personal information at the basis of their operation. Personal data gathered through a fairly typical user-login process may involve names and e-mail addresses, home addresses, credit card information etc. These data enable the operators of DRM e-commerce systems (the Content Industry or others) to establish a possibly "personal" relationship with users, creating their on-line "accounts" and completing payment processes through simplified steps. Unavoidably, these data also assist in imposing restrictions according to the DRM system's rules to the use of acquired content: for instance, iTunes connects users to home computers and allows for reproduction of purchased

content only on five computers per user. All these operations would have been impossible without the creation of user "accounts", whereby content purchased, hardware identification and other details are interconnected.

Nevertheless, collection of personal data will normally not go unchallenged in Europe (or, at least, in EU Member-States). According to the Data Protection Directive, "*processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage [...]*"[48]; and, accordingly, "*this Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*"[49]. It becomes therefore clear that the collection of personal information within DRM e-commerce systems does constitute an activity falling within the scope of the EU Data Protection Directive; the Directive has by now been implemented in all Member-States, constituting thus national law, and therefore each and every one EU Member-State, to which DRM e-commerce systems such as iTunes are addressed, now has to assess their rules according to its Data Protection legislation.

Collection and processing of personal information has to be performed "*fairly and lawfully*", collected information may be used only for "*specified, explicit and legitimate purposes and not [be] further processed in a way incompatible with those purposes*", it must be "*adequate, relevant and not excessive in relation to the purposes for which it is collected, accurate and, where necessary, kept up to date*"; in other words, in Europe DRM e-commerce systems will have to conform to all fundamental data protection principles[50]. Furthermore, the operators of such systems will most probably have to register with the Data Protection Authorities their creation of a filing system and processing of personal information. And, all these will have to be observed in each and every one EU Member-State locally (for instance, if iTunes sells to Greece, it has to register with the Greek Data Protection Authority and observe the Greek Data Protection Act – notwithstanding the fact that the Act is more or less the same as the Data Protection Directive).

Perhaps of more relevance to DRM e-commerce systems is the matter of international transfers of personal data. Although it is to be expected that all international DRM e-commerce operators are aware of and shall probably have allocated enough resources to comply with data protection requirements in all European states they aim to sell, where their infrastructure (servers) is located may be a totally different (and interesting) issue. Exports of EU personal information are only allowed under very strict rules: "*the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection*"[51]. There is no need to go into the details of the negotiations between American and EU authorities, assessing whether the American level of protection can be deemed "*adequate*" in order for data exports to be permitted[52]; instead, it is sufficient to be noted that, if the servers of a DRM e-commerce operator are located outside the EU and personal information of EU residents is collected there, then all requirements of the EU Data Protection Directive must be met, in order for such processing to be lawful.

Profiling, Data Matching and Other Marketing Processing Methods

Because DRM e-commerce systems are essentially business systems, maximizing profit constitutes evidently one of their major concerns. To this end they might be tempted to use personal information stored in them in marketing campaigns or processes to offer "personalized" services to their customers, with a view to increasing sales[53]. Or, they might be tempted to use customer personal information to combat piracy or even fraud or other lawful and worthy purposes[54]. Nevertheless, in all those cases to the extent that personal information of EU residents is being processed, the EU Data Protection Directive provisions shall have to apply (making the lawfulness of such processing questionable).

With regard to profiling (the creation of customer-specific profiles that record preferences based on purchases or Web browsing and the subsequent use of such profiles in order to promote services or goods deemed compatible), it ought to be noted that the (EU Data Protection Directive) finality principle requires that personal information be processed for "*specified, explicit and legitimate purposes and not [be] further processed in a way incompatible with those purposes*"[55]. In this context, personal information transmitted to a DRM e-commerce system operator by one of its clients in order to execute an on-line purchase is not clear that it may be used in order to create a profile for the same individual and forward to its inbox material particular to its perceived preferences. On the contrary, each client has to be informed, at the time he fills-in the form necessary for the purchase process, of the (legal) person that is collecting his data and the purposes for which such data shall be used. The most common way-out for DRM e-commerce operators shall be acquiring the individuals' consent (through, for instance, opt-in and opt-out boxes placed at the bottom of the relevant form), but it should nevertheless be noted that the lawfulness of such *opt-in* techniques is questioned in several EU Member-States.

The finality principle becomes even more relevant when DRM e-commerce operators use personal information of their clients for other, undoubtedly worthy, purposes: the combating of piracy or even the operation of their own DRM systems (by limiting uses per user). Again in these cases the finality data protection principle, at least in Europe, prohibits that stored personal data be put to any other purposes that the ones they were collected for in the first place. With regard to DRM e-commerce systems, obviously personal data will have been collected with a purpose of executing a purchase; whether these data may be used in order, for instance, to "tag" users and prohibit unauthorized use through DRM techniques of their purchased content (for instance, reproduction on other mp3 players) remains questionable. It is equally questionable whether personal information collected under DRM e-commerce systems may be used for the fulfillment of other lawful purposes, as is the combating of piracy: for instance, if a user has given his personal information to the Content Industry in order to purchase music within a DRM e-commerce system, the Content Industry is not unequivocally allowed to keep a file on this user (IP, personal details) in order to tag use over the Internet and identify potential acts of (content) piracy – here again, the principles of data protection on the fair and lawful use of personal information ought to be observed.

In view of the above, DRM e-commerce operators might find it useful to observe closely (European) data protection legislation while drafting and implementing their DRM techniques on EU residents.

Other Legal Concerns

As repeatedly discussed in this Chapter, DRM e-commerce systems constitute essentially business systems that, once the lawfulness of their existence has been confirmed by Intellectual Property (copyright)

Law, will have to be judged on an *ad hoc* basis. In this subchapter a brief analysis shall be undertaken on certain legal issues that were raised through the implementation in the market of contemporary DRM e-commerce systems, particularly with regard to EU law.

DRM E-Commerce Systems and Competition Law

Because DRM e-commerce systems may be equipped with the functionality to identify the location of users (customers), obviously based on their IP address, some operators (for instance, Apple) have used it in order to setup a country-specific sales system. For instance, users in the UK are guided to the UK-online shop and are allowed to purchase content only from it (evidently, at UK-specific prices). In this way the DRM e-commerce system operator benefits from currency exchange rates in a world that is artificially divided by its e-commerce system.

Such DRM e-commerce systems implementations *per se* hurt competition and international trade. Probably because they are based on single-user purchases, no formal claims have been raised so far against this "functionality". Nevertheless, this implementation does infringe EU law as well: because EU law aims at the creation of a common market, an e-commerce system that, based on DRM technologies, sells at different rates between Member-States of the EU unavoidably violates substantial EU Competition Law[56].

EU Law Requirements for E-Commerce Systems

Again within the EU, DRM e-commerce systems should be setup in order to conform with basic EU e-commerce legislation. Although these do not pertain to the core technologies of DRM e-commerce systems, they do affect the way they do business: a series of legal requirements, for instance, on information that should be readily provided to customers in on-line shops, on the execution of contracts on-line, or on the protection of consumers once a purchase has been completed indirectly affect DRM e-commerce systems – their implementation is mandatory, in order for their operators to lawfully use them in Europe.

THE FUTURE(?): WEB 2.0, IPTV, VOD AND OTHER MARKET (& RESEARCH) DIRECTIONS

DRM systems for the on-line or off-line world are evidently here to stay. Once basic Intellectual Property Law has secured their existence, they are still considered an invaluable (if not the only) tool for the Content Industry to make its products available in contemporary market conditions. The dissemination of broadband networks among users and the digitisation, by now, of every conceivable "work" in the intellectual property sense (music, movies, pictures) has made unavoidable a future whereby users in an international market exchange files of any size at an uncontrollable pace. More substantially, this situation is affecting the market itself: no more are CDs considered the prime source of revenue for the Content Industry or even artists: by the time these lines are being written practically all major labels have announced on-line systems of content sales[57], while, at the same time, popular groups and artists discover that money is to be made from now on mostly from concerts and other channels of distribution (and are quitting music labels in the process[58]).

DRM e-commerce technologies are essentially found in the middle of all this: the Content Industry advocates their widest possible use now more than ever, as a matter of life and death. Users are shopping around on-line providers for the one who offers the least DRM-infected content. And, e-commerce entrepreneurs keep pushing the technology further, through innovative business methods.

A number of fields may be identified where DRM technologies could play or are already playing a central role. Web 2.0 implementations is an obvious candidate: the Content Industry is increasingly annoyed at user-created content that uses extracts of copyrighted material (TV shows, films, music) without permission – DRM systems could present a solution, either blocking this altogether or creating an adequate way of compensation for the Content Industry (because today infringements cannot be counted, the Content Industry is usually settling with blanket, arbitrary agreements with e-commerce operators such as YouTube for all and any of their content used in their Web pages). IPTV implementations is another potential field for DRM systems exploitation: because the Content Industry has learned its lesson from the online provision of music, by now it only makes available its content in IPTV applications when strong DRM systems are in place – as long as broadband access increases, these systems shall also gain in significance. Evidently, the same applies to Video-on-Demand (VoD) implementations: a number of, mostly telecommunications, service providers, in their attempt to increase revenue after the demise of their voice earnings, have introduced VoD systems, whereby users, through a set-top box installed at their TV set, are able to download films: here again the Content Industry (namely, studios) is only making its content available whenever strong DRM systems are in place to protect it from unauthorised reproduction.

DRM e-commerce systems, regardless whether users like them or not, are here to stay: their existence is secured by law (copyright) and strong proponents (the Content Industry) and their future well-being is warranted by always-increasing e-commerce innovative business methods. Being essentially technology-neutral systems that, at their most basic functionality, only protect content from unauthorised reproductions, it remains to be seen whether the business models they are put to serve shall alienate them from the public (that misguidedly identifies them as the problem) or shall integrate them effortlessly into an environment aiming towards ubiquitous computing, where, however, authors too have to make a decent living.

REFERENCES

Maillard, T., & Furon, T. (2004). Towards digital rights and exemptions management systems. *Computer Law & Security Report, 20*(4), 281-287.

Morin, J-H. & Pawlak, M. (2007, July 1-5). A model for credential based exception management in digital rights management systems, Internet monitoring, and protection. *ICIMP 2007. Second International Conference,* 41. Digital Object Identifier 10.1109/ICIMP.2007.3

Park, Y., & Scotchmer, S. (2005, August). Digital rights management and the pricing of digital products. *NBER Working Paper, W11532.* Available at SSRN: http://ssrn.com/abstract=778105

Tehranian, J. (2002, November). All rights reserved? Reassessing copyright and patent enforcement in the digital age. Available at SSRN: http://ssrn.com/abstract=351480 or DOI: 10.2139/ssrn.351480

WIRED (2006, April 3). Reasons to love open-source DRM. Available at http://www.wired.com/entertainment/music/commentary/listeningpost/2006/04/70548)

ADDITIONAL READING

Fairfield, J. (2005). Virtual property. *Boston University Law Review, 85*, 1047. Available at SSRN: http://ssrn.com/abstract=807966

Lessig, L. (2006). *Code version 2.0*. Basic Books

Zittrain, J. (2006, May). The generative Internet. *Harvard Law Review, 119*, 1974. Available at SSRN: http://ssrn.com/abstract=847124

ENDNOTES

1 See also Petrick, Paul, Why DRM Should be Cause for Concern: An Economic and Legal Analysis of the Effect of Digital Technology on the Music Industry (November 2004), *Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-09*. Available at SSRN: http://ssrn.com/abstract=618065

2 The Statute of Anne.

3 For a concise analysis, see Lloyd, I. *Information Technology Law*, Oxford University Press, Fourth Edition, pp.363ff.

4 While not being particularly discomforted at that time by what essentially was computer-copying the Content Industry suffered a serious blow in another field and thus learned a lesson that proved invaluable in the very near future: VCRs. During the 80ies the VCR technology became immensely popular: for the first time in human history non-expert home-users at a minimum effort and cost could copy and reproduce at the ease of their home valuable copyrighted material (films and other TV material). The Content Industry reacted to such technology and sued those who profited from it, namely SONY Corp. After bitter and long court struggle, in the milestone SONY/BETAMAX case video copying was ruled lawful (see below, footnote 10). The flaws of the Content Industry in that case proved of invaluable importance a few years later, when P2P networks came into play. The Content Industry ultimately won this battle, not least because it did not step into the traps of the BETAMAX case (while the P2P industry seemed poised to do so).

5 See also Petrick, P, *ibid*.

6 See Zittrain, J, The Generative Internet, *Harvard Law Review*, Vol. 119, p. 1974, May 2006, available at SSRN: http://ssrn.com/abstract=847124

7 Now transformed into fee-based service, at www.napster.com.

8 Court of Appeals (Ninth Circuit) 380 F 3d 1154.

9 *Sony Corp. of America v. Universal City Studios Inc*. 464 US 417 (1984, *BETAMAX case*).

10 *Metro-Goldwin-Mayer Studios Inc. et al. v. Grokster Ltd., et al.,* 27 June 2005.

11 See IFAA press articles.

[12] P2P technology was nevertheless under no circumstances abandoned. A similar implementation may be met today in networks such as Skype. This evidently does not include any content exchange; when P2P networks did become again involved in content exchange, this time it was done with strict observation of copyright rules (and with full implementation of DRM systems, see, for instance, Joost at www.joost.com).

[13] On "content" see also WIPO, Standing Committee on Copyright and Related Rights, *Automated Rights Management Systems And Copyright Limitations and Exceptions*, April 27, 2006 (SCCR/14/5), p.13.

[14] Probably confirming Lessig's assertion that "code is law" (Lessig L, *Code version 2.0*, Basic Books 2006).

[15] Also see, however, David Weinberger, *Copy Protection is a Crime against Humanity: Society is based on bending the rules*, at WIRED, http://www.wired.com/wired/archive/11.06/view.html

[16] For a broader analysis of typical (at least contemporary) DRM e-commerce applications see *Center for Democracy and Technology*, September 2006 (version 1), pp.8ff., available at www.cdt.org/copyright/20060907drm.pdf, pp.8ff.

[17] See also Gasser, Urs, iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media - A Case Study (June 2004), *Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-07.* Available at SSRN: http://ssrn.com/abstract=556802

[18] See, The Economist, Music wants to be free, February 8, 2007 (available at http://www.economist.com/opinion/displaystory.cfm?story_id=8668981).

[19] Terms found at http://www.apple.com/legal/itunes/uk/service.html/

[20] See WIRED, *The year of living DRMishly*, January 24, 2006 (available at http://www.wired.com/science/discoveries/news/2006/01/70049)

[21] See *Evaluating DRM: Building a Marketplace for the convergent world*, pp.5ff.

[22] Felten, E *DRM and Public Policy* in Communications of the ACM, V. 48, No. 7, July 2005, p. 112, but also see WIPO, Standing Committee on Copyright and Related Rights, *Automated Rights Management Systems And Copyright Limitations and Exceptions*, April 27, 2006 (SCCR/14/5), pp.17ff.

[23] See WIPO's official site at www.wipo.org.

[24] See the, essentially identical, texts under http:// www.apple.com/legal/itunes/ww/.

[25] Its provisions, with regard to DRM at least, have been implemented in the USA through the Digital Millennium Copyright Act (DMCA), and in Europe through the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (EU Copyright Directive).

[26] Art. 11 WCT.

[27] See, for instance, the, largely legalistic, argumentation whether TPM that can be circumvented can be "effective" or not, in order to infer whether they are protected by the WCT (see, however, Art. 6 par. 3 of the EU Copyright Directive, and, recently, *Helsinki District Court Decides That CSS Used in DVDs Is "Ineffective*, International Law Office Information Technology Update, available at http://www.internationallawoffice.com/Newsletters/Detail.aspx?g=c720e545-425b-4f73-93de-cf2ed7638764).

[28] After all, the regulation of TPM is as far as Intellectual Property Law is allowed to go. DRM systems constitute "systems" that regulate the use of content. As such, only their case-specific rules for such use may be assessed (on an ad hoc basis) according to Intellectual Property Law

provisions (see, for instance, the *fair use* principle, wherever applicable). This assessment of their rules does not refuse DRM systems their right to exist (perhaps, using other rules). Intellectual Property Law deals with works, and the act of attaching TPM onto them, thus amending them, is an act that may or may not be accepted as such under its provisions. Once it is established that attaching TPM onto works is lawful, self-evidently some (DRM) rules for the use of this TPM content are to be expected.

29 See Art. 6 of the European Directive on the legal protection of computer programs (91/250/EEC)

30 Article 6.4.

31 See US Copyright Office under http://www.copyright.gov/fls/fl102.html, and the respective entry in Wikipedia under http://en.wikipedia.org/wiki/Fair_use .

32 In the DRM context see Reinbothe J, *Private Copying, Levies and DRMs against the Background of the EU Copyright Framework*, available at http://ec.europa.eu/internal_market/copyright/documents/2003-speech-reinbothe_en.htm .

33 See, however, The Economist, *Criminalising the Consumer*, April 27, 2007 (available at http://www.economist.com/science/displaystory.cfm?story_id=9096421).

34 Naturally, it is a totally different issue if, for instance, implementation of a DRM system eventually harms hardware or software owned by the user. Although this has nothing to do with copyright law examined here, evidently the owner of the DRM system shall be fully liable to indemnify the user for any damage suffered while using lawfully acquired content (see also Evaluating DRM: Building a Marketplace for the convergent world, p.20).

35 Berne Convetnion, Art. 6bis par. 1.

36 See, for instance, the iTunes Terms of Sale: "iTunes Plus content does not contain security technology that restricts your usage of such content, and is encoded at a higher audio bit rate than the DRM-protected songs or music videos available on the iTunes Store" (under http://www.apple.com/legal/itunes/uk/sales.html).

37 See WIPO, Standing Committee on Copyright and Related Rights, *Automated Rights Management Systems And Copyright Limitations and Exceptions*, April 27, 2006 (SCCR/14/5), p.13.

38 See Evaluating DRM: Building a Marketplace for the convergent world, p.21.

39 See, however, WIRED, *Reasons to love open-source DRM*, April 3, 2006 (available at http://www.wired.com/entertainment/music/commentary/listeningpost/2006/04/70548)

40 Art. 6.1, European Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

41 See also Center for Technology and Democracy, *Evaluating DRM: Building a Marketplace for the convergent world*, pp.15ff.

42 http://www.focus.de/digital/multimedia/ipod/apple_aid_50327.html

43 The Ombudsman ruled that that the terms of the iTunes License Agreement (in its then version of 2006) were "unreasonable" with respect to the Norwegian Marketing Control Act, that it was unlawful to submit the License Agreement to English law, as well as, that the same Agreement's disclaimer on Apple's liability for possible damage its software may cause was equally unlawful (see http://forbrukerportalen.no/Artikler/2006/1149587055.44 , and also http://www.out-law.com/page-7691).

44 See, among others, the EDRI relevant entry at http://www.edri.org/edrigram/number5.1/drm_sonyfr. It should also be noted that France has provided for an "Authority for DRM" to be established under its DADVSI Act

45 As per Electronic Frontier Foundation (EFF)'s description, "at issue are two software technologies - SunnComm's MediaMax and First4Internet's Extended Copy Protection (also known as XCP) - which Sony BMG claims to have placed on the music CDs to restrict consumer use of the music on the CDs but which in truth do much more, including reporting customer listening of the CDs and installing undisclosed and in some cases hidden files on users' computers that can expose users to malicious attacks by third parties, all without appropriate notice and consent from purchasers. The CDs also condition use of the music on unconscionable licensing terms in the End User Licensing Agreement (EULA)" (http://www.eff.org/cases/sony-bmg-litigation-info).

46 See Evaluating DRM: Building a Marketplace for the convergent world, pp.19ff.

47 See Coher J, DRM and Privacy, *Berkeley Technology Law Journal*, available at https://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html

48 Art. 2b, EU Data Protection Directive (95/46/EC).

49 Art. 3.1, EU Data Protection Directive (95/46/EC).

50 Art. 6.1, EU Data Protection Directive (95/46/EC).

51 Art. 25.1, EU Data Protection Directive (95/46/EC).

52 On this issue see the official EU site at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

53 See Kerr, Ian R. and Bailey, Jane, The Implications of Digital Rights Management for Privacy and Freedom of Expression, *Journal of Information, Communication & Ethics in Society*, Vol. 2, 2004, Troubador Publishing Ltd. Available at SSRN: http://ssrn.com/abstract=705041

54 In this context it should be noted that, at least in Europe, the notion of "personal information" largely exceeds the routine use of the term in everyday life, in order to include any piece of information that may have even a remote connection to an individual – for instance, IP addresses, even if not connected to users, do constitute "personal information" for the purposes of data protection legislation in Europe (see Working Party Opinion 4/2007).

55 Art. 6.1, EU Data Protection Directive (95/46/EC).

56 See COMPUTERWORLD, *Apple drops iTunes prices, EU drops antitrust action*, January 9, 2008 (available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9056458)

57 See WIRED, *Death of DRM could weaken iTunes, boost iPod*, January 4, 2008 (available at http://www.wired.com/entertainment/music/news/2008/01/rip_drm)

58 See The Economist, *Online Music: The slow death of digital rights*, available at http://www.economist.com/business/displaystory.cfm?story_id=9963252