Digital Rights Management

Lyudmila Vaseva
Institute of Computer Science
Freie Universität Berlin, Germany
vaseva@inf.fu-berlin.de

***Abstract*—The topic of digital rights management technologies becomes more and more important for the modern society. Since technology is constantly developing and the numbers of consumers are growing, it is not surprising that people want and should be more aware of what their rights and obligations in the high-tech world are.**

This paper outlines what DRM[1] technologies are, where they are applied(based on specific examples), and how it has come to their development at all. It then moves on to examine the topic from the technical, legal, and philosophical point of view. Furthermore, it is explained how companies implement DRM—on software and hardware level, and some ways to bypass it are presented. Afterwards, alternative strategies to deal with copyright issues are briefly discussed. At the end, the paper summarizes benefits and drawbacks of the technology for all parties concerned. It compares the concepts of both defenders and opponents of the idea drawing the conclusion that freedom of speech, work, and mind must prevail.

I. Introduction

Digital Rights Management is a major issue concerning all of us. One look at the recent press publications shows us clearly that the topic is part of our every day lives.

> *"Microsoft sets sights on CD piracy"*
>
> Microsoft has released new software aimed at helping the music industry stop piracy of CDs [...] The music industry has been trying out different technologies to stop the unauthorised copying of CDs but most have been cracked or have annoyed customers [...] Record labels are increasingly concerned about music piracy, blaming a drop in sales on song swapping online [...] The software giant has invested $500 million in digital rights management technologies as this is seen as the way to stop music piracy [...] Other companies such as Sony and Real Networks are also looking to build a business out of securing copyright protections across the internet and other digital media.[2]
>
> *"CDs that do not play"*
>
> These short excerpts evidently demonstrate the importance of the topic and the fact that it interests the society. The paper will try to outline what DRM actually is, where and how it is applied, and what the possible advantages/drawbacks for all the parties concerned are.
>
> A consumer in France bought a CD distributed by EMI, one of the major music publishers. At home, he discovered that he was not able to play the CD on the computer or in his car's CD player. As he learned later from a friend, this has to do with electronic copy protection technology, a so called Digital Rights Management (DRM) system that EMI used on the CD.[3]

Digital Rights Management can be defined as a set of technologies which aim at supervising and managing the use of digital intellectual property. Hereby is meant exclusively the technical implementation of these technologies and it should not be mixed up with the legal side of the issue, summarised in the section III of the current paper. "Digital intellectual property" generally concerns audio and video CDs and DVDs, online music and videos, E-Books, and images [1]. The primary idea is to restrict unauthorised use of the data—which can be copying, printing, changing the contents, viewing by certain individuals. The impact of these technologies is diverse. It can include data expiring after a certain period of time, data expiring after a certain number of times viewed, data limited to a certain number of devices it can be used on, restriction of converting data to other digital formats, restriction of data editing, ban of copying to clipboard and distributing, ban of printing. In many cases, specific hardware is needed in order to

[1] DRM stands for Digital Rights Management

[2] From: BBC NEWS, 20.01.2003, http://bbc.co.uk

[3] From: Natali Helberger: Thou shalt not mislead thy customer! INDICARE Monitor, Vol. 2, No. 9, 25.2.2005, http://www.indicare.org

gain access to the data at all. For example the music you purchase at the iTunes online music store can be played on no other portable music player but on an iPod. In the whole process there are three parties involved—the author/the rights owner of the product, the license creator (the company which creates and implements the DRM technology), and the end user. The consequences (both positive and negative) these technologies have for each of the groups concerned are discussed in section IV [2].

But how come we need copyright protection technologies at all? Computer games are one of the earliest examples where DRM technologies have been applied. In the 1980s there were various and often truly creative methods to restrict the unregulated use of the games. One of the most popular approaches was asking questions similar to: "What is the 7th word on the 10th line of page 17?" The aim was to make sure that the player had the original manual, i.e. that had actually bought the game. Sometimes, in the original package there was a specific guide or other material providing vital information without which the player could not make progress in the game. In the remote 1984 Firebird Software released the game Elite. In each package there was additionally a small plastic device containing two prisms called lenslok [3]. The player was not able to start the game without the device—at the beginning on the screen appeared a special code, which was corrupted by switching the vertical bands of the image. The correct two letters word could be read only with the right lenslok, which was able to rearrange the vertical bands and display the original image. Back in the 1980s that simple mechanism was one of the first examples of using copyright protection technologies.

Then, in 1990s with the spreading of the Internet for home use, the virtual piracy spreading, and, eventually, the peer2peer boom the demand for such technologies rose. It became way easier to circumvent copyright laws, causing great intellectual and financial losses for authors of copyrighted works. From their point of view it was clear that something stricter than a copyright law was needed, something that can make people actually obey this law. However, if DRM systems are actually the best solution for authors themselves is also disputable—as shown in section IV.

The question of defining DRM is now answered. Still, that opens many new problems, some of which will be discussed in the rest of the paper.

The core of the seminar topic is introduced in section II. It deals with where can DRM be found, how is it implemented (on both software and hardware level), and eventually, how can it be bypassed. Section III continues with a brief discussion of the legal side of the topic and the possible alternative solutions. Afterwards a sound comparison of the positive and negative aspects of the technology for each of the sides concerned is done in section IV. The paper closes with a conclusion in section V.

II. Insight

This section of the paper focuses on the application scenarios of DRM technologies and discusses examples for the implementation of such technologies. Then it explains how they can be implemented and finally also mentions the ways in which these technologies can be bypassed.

A. Where Are Examples For DRM Found?

We can divide the cases in which DRM technologies are used in the following categories:

1) Online Music/Videos: One of the wide spread examples for data where DRM protection technologies are used are online audio and video files (or at least, legally available online audio and video files). That is also logical, because the distributors need a way in which they can prove whether the user has bought the license for the product or not. We can find DRM systems in the Apple's iTunes store, the Napster online music shop, the German Telecom's Musicload online music store, Yahoo! Music, etc.

In the case iTunes the implications of the DRM technologies for the user are: The only portable music player which you can use to play the music is an iPod. You are able to copy the downloaded music on up to 5 computers and unlimited number of iPods. If you wish to play the music from CDs you own on your iPod, you should extract it with the special iTunes' software. You are also able to burn the iTunes music on a CD. Apple uses the Advanced Audio Coding format (AAC), which protects the audio data inside the file by encryption [4] [5].

If you choose to be a customer of Musicload and buy their DRM protected music, you will be allowed to burn it on a CD or transfer it between your computer and portable music player only in case you have the valid license as well. This is a second file you receive along with the music file when you purchase the track. You also need the license in order to play the music at all. Your system and portable devices must be DRM compatible and the whole scheme works only under Windows. Musicload uses the Windows Media Audio (WMA) and Windows Media Video (WMV) formats [6].

2) Audio and Video CDs/DVDs: DRM technologies are also used to prevent you from copying your audio or video CDs and DVDs or from playing them under some conditions. Maybe the most obvious example in this case is the region coding of DVDs. According to it, the world is divided into 6 regions. For each region the main part of the sold DVD players are specified so (using firmware to set a configuration flag) that they cannot play DVDs bought in other regions. Exception are the region 0 discs, which have no restrictions and can be played everywhere. This way a media publisher can set different marketing policies in different regions, alter prices, release date, included content, etc. Among DRM critics arise the concerns that such strategy violates user rights, because users often cannot take advantage of media they have legally obtained. However, it is relatively easy to work around a region code, since there are region-free DVD players, possibilities to reset the factory-set configuration flag and programs developed to crack the coding. Some DVD player manufacturers even distribute freely the information how to bypass the regional coding.

Currently arising technologies like the Blu-ray disc and the HD-DVD take a great advantage of DRM systems as well. You need a TV which supports digital encryption via a HDMI[4] [7] port or an HDCP-compliant[5] DVI port. If you wish to watch the Blu-ray disc on your PC, your video card and monitor should be HDCP-compliant as well. Additionally, you can be charged money for making backup copies and your player should be connected to the Internet in order to play the disc. Furthermore, Blu-ray discs and HD-DVDs are generally not compatible with free software, so they cannot be run on systems which do not use Windows or Mac OS [8].

3) E-Books: E-books are another media type which uses DRM protection technologies aiming to limit the copying, printing, and sharing of the data. E-books are usually limited to a certain number of reading devices (PCs or portable readers) and often any copying or printing is forbidden. There are different approaches used to reach this objectives. Sometimes the data is bound to the specific hardware architecture (to the specific device), sometimes it is bound to the user [8]. In order for these measures to be applied and managed, different software products are used. The most popular of these are the Adobe Acrobat Reader and the Microsoft Reader.

Using Adobe Acrobat Reader you are able to read both DRM protected and DRM free documents. You can easily find out what the specific restrictions (if any) applied to the certain file are by selecting Document properties/Security. With Adobe Acrobat you can control the printing, copying (of the whole document as well as of parts of the document), commenting, signing, document assembly, and other properties of the work you create.

The Microsoft Reader divides the E-Books in three categories corresponding to the level of protection. In the case of Sealed E-Books the user cannot modify the content of the file. That guarantees that the work you have received is genuine and prevents plagiarism. Additional feature of the Inscribed E-Books is displaying information for the purchaser (for example the name) on the front page of the document. It is assumed that the user will be more reluctant to broadcast a work where his name appears as owner in the document over Internet. In some cases, not only the name of the owner but the number of his credit card is also displayed and he needs both in order to get access to the file on the first place. The third category are the Owner Exclusive E-Books. Here you need an additional encrypted license in order to activate your computer for the Microsoft Reader and only then you can purchase and read the Owner Exclusive E-Books. Copying parts of these books in other applications is not allowed. It is important to mention that when using Microsoft Reader, unlike the Adobe Acrobat Reader, one cannot easily see which protection properties a specific work has [9].

4) Software: games, financial software, other products

The last category of products where DRM technologies are used is software. The most popular example are probably computer games. However, this applies to all kinds of programs which are not issued under a Free Software license, like picture and media processing software, dictionaries, encyclopedias, etc, and most importantly, financial and other kinds of corporative software. In the case of computer games and other programs aimed at the average consumer the goal is preventing the use of the product for people who have not bought the license. Measures such as copy prohibition (or hindered copying of the source, so that afterwards the copy is unreadable), the requirement of the original CD/DVD in your CD or DVD-ROM drive to run the program and, of course, protection of the product with a license key are often used. In the simplest version you get the key at the purchase of the software. In the case of the AutoCAD design application for example, you get

[4] "High-Definition Multimedia Interface provides an interface between any audio/video source, such as a set-top box, DVD player, or A/V receiver and an audio and/or video monitor, such as a digital television (DTV), over a single cable."

[5] High-Bandwidth Digital Content Protection, "a copy protection scheme to eliminate the possibility of intercepting digital data mid-stream between the source and the display."

one key at the purchase. Then you have to register your copy online and get another key in order to actually run the software. For professional products such as money transfer managing suites etc, it is naturally essential to ensure that no unauthorised use of the product and alteration of the data occurs. Consequently, digital rights are managed through a complicated system of passwords, authentication keys, integrity checks etc [10].

B. How Are DRM Technologies Implemented

Generally, the whole scheme behind every DRM system consists of two parts—protecting the licensed content somehow and authenticating the user who has bought this license, so that he can unlock the content and use it. Basically, we can say that the data is put in a secured container, which can be opened only by a rightful user. Usually, the securing consists of scrambling the data by an encryption algorithm/method in some way. If there is no valid authentication, the user cannot unscramble the content correctly and consequently, cannot view it. There are many protection approaches such as diverse encryption algorithms, watermarking, fingerprinting on the software side and unconventional writing on the media platform, trusted computing on the hardware side. The authentication process is needed in order to ensure that only rightful users get access to the information. Sometimes however, mere identification is not enough. There are DRM systems which prevent access to the data not only when authentication fails but also if the decryption has already occurred too many times (example here are video or music files, limited to a certain amount of viewings) [2] [11].

1) The Software Approach:

a) Watermarks: A digital watermark is a piece of identification code/bit string embedded in the digital work. It has to be invisible for the human eye and robust enough to remain unaltered after changes to the file or conversion into analogue form. It usually contains some information about the author (allowing illegal copies to be traced) and causes disturbance (like for example distortion for video and audio signals) when unrightfully alternated/copied content is displayed. Using watermarks the author of the digital works can (theoretically) trace all illegal copies distributed on the Internet and act in accordance. A digital watermark should also be designed so that it is as difficult as possible to remove it without harming the content. To achieve this, license creators scatter the bits of the watermark throughout the whole file, rather than placing them all together at one spot [12].

b) Fingerprinting: The digital fingerprints are, similar to digital watermarks, pieces of identification information embedded in the digital work. However, unlike the watermarking approach, in the case of digital fingerprinting each copy of the work receives an unique code which helps identifying its owner and trace those responsible for illegal distribution of content. Fingerprints are used not only as a DRM technology but often also as a tool to find contents similar to the one bearing the fingerprint. In these cases the fingerprint contains pieces of characteristic for the media file information. For example, in case of audio files are compared parameters such as frequency, pitch, rhythm, and of video files—visual content, colours, movement and frames [13] [14].

c) Encrypting: One popular way to protect digital content is encryption. Generally, some algorithm is used to code the information, making it useless for people who do not possess the right key to decode it. The types of encrypting are primarily two. The symmetric key encryption is an approach where all the people/devices which are going to swap encrypted information should have the key in advance. In the case of asymmetric key encryption each of the communicating parties has a public and a private key. Users wishing to send an encrypted message to a particular person encrypt it using receiver's public key, which is visible for everyone, and afterwards the person is able to decode and read the information via the private key. In diverse cases authentication can take place through passwords, digital signatures, certificates [8]...

In the case of the SWIFTAlliance financial communication software are used numerous keys for identification of the user, as well as database and software integrity checks every time information from the database is read or modified. The verification happens using CRC (Cyclic Redundancy Check). The calculated value is each time compared to an expected value (trusted value) and in the case of a mismatch an error event is recorded in the event journal and the process is not started. This ensures that inter-process communication only takes place between genuine SWIFTAlliance programs. It additionally keeps a record of the logged on users and the alternations made. This approach vastly decreases the probability of unauthorised data modification occurring, but does not protect the data against deletion (deliberate or accidental). To ensure that this will not happen, SWIFT have implemented an input/output sequence number permission for all messages allowing deleted/lost messages to be identified [15].

2) The Hardware Approach:

a) Copy Protection Through Unconventional Use Of CD Tracks At Manufacture Time: Each sector of a CD-ROM contains some structural information. Part of it are the number of the sector, the relative and the absolute logical position of the sector, the Error Detection Code

(EDC) and the Error Correction Code (ECC). Some manufacturers append additional EDC/ECC fields alternating with proper content. They do not contain information about real errors, and thus are interpreted as unreadable sectors. When told to duplicate the media, the burner thinks that the whole interval of sectors is corrupted and skips it at copying.

Each CD-ROM contains also several sub-channels where normally meta information is stored. Some CD copy protection schemes use these sub-channels to store additional information in them, allowing distinction between original and copies.

Another idea is using twin sectors. This refers to including sectors with duplicating numbers which contain different information from the one saved in the initial sector with the same number. When copying such discs, the software skips the second sector with a specific number, because after each sector it looks for its successor. Thus, it can be checked whether the disc is original because copies do not contain the twin sector. (In the original version, when playing forwards the first of the twin sectors is found, when playing backwards - the second.)

b) Dongles: Another technology used to lock content for unrightful users is the dongle. That is a piece of hardware with an unique electronic serial number which has to be plugged in in one of the I/O ports of the computer, so that the digital content/software can be used. Nowadays, the most popular implementation of the technology are the USB dongles. However, they are not particularly widely spread because manufacturing them adds extra cost to the product, so they are applied mostly in cases of expensive “high-end” software packages [8].

c) Trusted Computing: User space/user platform where the DRM protected data should be executed is viewed as a hostile territory. Consequently, secure environment on the user side is needed to guarantee that the data remains protected. This secure environment is referred to as “Trusted Computing Base”. It can be viewed as a resource reserved for the product distributor. Tasks performed in this environment cannot be inspected or disturbed by the user. Trusted computing provides the following features: Secure input/output communication ensures that there is no foreign interference in the communication between the user and the program. Memory curtaining denies access to parts of memory where encryption keys and other security information are stored. And sealed storage which means that digital data can be accessed only with the right combination of hardware and software, not allowing you for example to play music tracks you have on your hard disc drive if you have not obtained the license for them.

However, despite the fact that the user is actually the owner of the platform where the trusted environment is generated, he has no rights to manage this part of the system. It shall obey exclusively to the content distributor. Trusted computing can prevent you from running software the system has considered insecure. The aim is restricting piracy and virus distribution, but on the same time it prevents you from actually execute your tasks and use your PC properly in the way you want to. It also violates user’s anonymity.

Another common implementation solution is tying the content to a device or a person. In the first case some information about the user’s PC or portable player is used for the authentication—for example the number of the CPU or the MAC address of the Ethernet card. This approach has obvious disadvantages for the final user. If exactly this part of the system which is used for authentication crashes irrecoverably and needs to be exchanged or the user wants to upgrade his hardware the digital data becomes unusable. A more user-friendly strategy is tying the content to the user himself. I.e. some special information which can be provided only by a rightful user is used for the authentication. For example that can be the user’s credit card number, which he will be most likely reluctant to distribute in the public space so that other individuals may gain access to the data as well [9] [10].

C. How Can DRM Technologies Be Bypassed

1) Analogue Hole: This notion describes the fact that any audio-visual media should sooner or later be converted to an analogue form so that it can be perceived by our senses. And once the media has been turned into an analogue form, it can be recorded again in the simplest possible way—using camera and/or microphone. Of course, that means a loss of quality, but often it does not matter. No matter what the quality is, it is preferred having the data in a bad condition to not having it at all. That is why, this is a way still used to make unlawful copies of media. And a way that can always be used.

There are also measures aiming to discourage analogue recording. They alternate the signal in such a way that it can interfere with or confuse some recording devices. For example, they can output a deliberately distorted video signal, so that it disturbs the automatic gain control for videos, which results in brightness fluctuations. However, this approach is unreliable because sometimes this effect occurs not only to copies but to the original as well. Moreover, there are devices which are able to counteract this measure [8].

2) Ripping: Using special software in the majority of the cases the user is able to rip the content of a music or video CD/DVD on to his computer. The term ripping refers to the extraction of the content of CDs or DVDs onto the hard disc drive of the computer. It is not a synonym of copying because ripping often includes format encoding/shifting and/or surmounting of copy protection mechanisms.

3) Key Generators: Yet another way to get access to the content of a DRM sealed data (without actually buying the license) is using the so called key generators. They can be applied in the cases in which you need a special code sequence (i.e. key) to open the DRM protected data. The working principle of a key generator is simple. Somebody deciphers the characteristics of a valid code sequence or the algorithm in which valid keys for the product are generated. Then, this person writes a small program the task of which is to generate sequences fitting to these characteristics.

As we can clearly see, there are numerous ways to get past the DRM measures. So, inevitably, the question arises: "Is it at all worth it to invest the money, time and efforts in developing DRM systems?"

III. Legal aspect

A. DRM Technologies vs Copyright law

Copyright law consists of the set of legal regulations concerning the rights and obligations of users of copyrighted material. They describe what uses of such materials are allowed and what the possible consequences for law breaking are. Like all laws, they themselves do not implement anything, they just inform and warn. In contrast to these laws, DRM technologies actually implement the rights of the user. The copyright law may forbid copying of the work. However, whether you do it or not is left to your conscience and possible fear of punishment. A DRM technology will actually make it technically impossible for you (to some extend or another, as already mentioned in section II) to copy the work. Consequently, some people defend the thesis that, where copyright law is an expression of "everything that is not forbidden is permitted," DRM takes the approach of "everything that is not permitted is forbidden." When DRM system is implemented, any action you want to take, has to be explicitly granted.

However, it is false to think of DRM systems as a way to implement Copyright Laws, since the regulations of these laws and the implementations of the systems usually do not overlap each other identically. It is better to think of DRM systems as systems for the protection of digital works.

At the moment the situation in the world is the following. In Europe the regulations of the EU Copyright Directive from 22.05.2001 are in force In the United States operate these of the Digital Millennium Copyright Act, which among other things criminalises the production and dissemination of technology that allows users to circumvent technical copy-restriction methods [16] [17] [18].

However, many of the users and some lawyers argue that DRM systems do not just implement copyright laws but exceed their regulations. For example in the legislation of many European countries it is allowed to make copies of audio or video materials for "home use". There are many cases in which possessing an extra copy of the work may indeed be in handy—if the platform of your original copy gets irrecoverably damaged, if you want to make a copy of a video cassette for your children, who anyhow eventually break everything. The problem is, sometimes DRM systems prevent you from taking advantage of this lawful right of yours, as copying is technically impossible. That is why many people rather disapprove of these technologies. The intrusion of the consumer's rights by the DRM technologies is not limited to just this one case. In this category falls the regional coding as well. You are not allowed to play in Germany a DVD you have bought in the USA, although you have paid for the good and you are its rightful owner. What is more, no matter that you own both the DVD and the DVD player, if you break the regional coding in order to use your DVD somewhere else, you are breaking the anticircumvention[6] laws. No matter what the license imposing companies may claim, such a measure has for sure nothing to do with the protection of digital data. It is only a way for retaining monopoly and making money. In fact, it is a rude violation of the consumer's rights. Not that this fact has prevented them of implementing the strategy. Moreover, according to the Electronic Frontier Foundation, region coding is a way "to discriminate against poor countries by offering them information goods only after they have exhausted their commercial potential in rich countries". A claim which, unsurprisingly, wins a broad popularity [2] [9] [19].

Furthermore, DRM systems often need their own set of laws so that they could actually operate. Researchers of the EFF claim that DRM systems are often so imperfect that they fail to reach their objectives and protect themselves and need the so called "anti-circumvention"

[6] Here is how anticircumvention works: "if you put a lock – an access control – around a copyrighted work, it is illegal to break that lock. It's illegal to make a tool that breaks that lock. It's illegal to tell someone how to make that tool. One court even held it illegal to tell someone where to learn how to make that tool."

laws to silence researchers who discover their flaws.

B. Alternative Law Solutions

In order to avoid all these complications and not to violate users' rights, to encourage creativity and distribution of the works and still preserve author's rights, there were more than one alternative solutions to the Copyright License developed. The most significant examples are the GNU General Public License (GPL) and the Creative Commons License.

The simplest way to surmount all the DRM technologies and making a software/digital data free is just to release it in the public domain without bounding it to any kind of license. However, that is probably not the wisest decision, since anybody can make whatever modifications to the product he/she desires and then release it again, but this time as a proprietary software. That is why licenses like GNU GPL and Creative Commons are used.

In short, GNU GPL grants you as user the freedoms to

1) use the program as you wish;
2) study the source code and modify it to do what you wish;
3) make and distribute copies, when you wish;
4) and distribute modified versions, when you wish.

Furthermore, it protects these freedoms for all users of all versions of the program in question by forbidding middlemen from stripping them off [20].

Creative Commons license is another alternative approach concerning issuing and spread of digital media. It appears in several possible forms - use under:

1) Quoting the name of the author
2) Quoting the name of the author + no editing
3) Quoting the name of the author + using for no commercial purposes
4) Quoting the name of the author + using for no commercial purposes + no editing
5) Quoting the name of the author + using for no commercial purposes + spreading under same conditions
6) Quoting the name of the author + spreading under same conditions

It further allows personal contracts between copyright owners and users in single cases [21].

IV. Evaluation

In this section I take a look at different opinions on the issue and subsequently, draw up the positive and negative impacts of the DRM technologies for the different parties concerned.

A. Opinions

1) Bill Gates and Microsoft: Bill Gates spoke about DRM at Consumer Electronics Show (CES) in 2006. On his account, DRM in its current state is not beneficial for the end users. Trying to differentiate between legal and illegal users, it causes problems for the fair consumers and he is rather against it in this form. Nevertheless, Microsoft has developed the Windows Media Rights Manager SDK[7] DRM system enabling content providers to distribute their data securely over the Internet using encrypting. These files can be either streamed or downloaded to the consumer's computer [22].

2) Steve Jobs and Apple: Apple wanted to distribute music legally over the Internet. The music companies agreed to sign a contract, on the condition that Apple offered an adequate protection of their data, i.e. that Apple guaranteed that it would not be possible that the copyrights of the works were violated. In order to offer the service to legally download music from the Internet, Apple had to protect the tracks with the DRM technology developed by themselves.

Further on, according to Steve Jobs, Apple opposes DRM music and has even issued a public letter calling its music labels to stop requiring DRM on its iTunes Store [23]. Today, EMI has agreed and Apple has developed iTunes Plus. It offers DRM free music and the option for the consumers to update their tracks to the new version (if the tracks are available in this new version) by only paying the difference between the old and the new price. The old service offering DRM secured music remains. However, DRM on video content is considered as a separate issue by the company.

3) Cory Doctorov: According to Cory Doctorov[8] in his Microsoft Research DRM talk from 17.06.2004 DRM, systems fail to reach their objectives on many fronts.

To begin with, he defends the position that DRM systems do not work anyway, because they get sooner or later cracked. All the crackers need is the cypher text and the key, and they can obtain them both. Anyone can surmount DRM technologies without being a computer genius. The person just needs to be able to use Google or other general purpose search engine for the information somebody else has extracted.

Moreover, Doctorov gives a social reason for the failure of the DRM technologies - “keeping a honest user honest is like keeping a tall user tall”. The technologies

[7] SDK stays for Software development kit

[8] Cory Doctorov is a science fiction writer, European Affairs Coordinator for the Electronic Frontier Foundation, co-founder of the Open Rights Group and strict opponent of the DRM technologies

are surmountable and honest consumers are going to buy the good anyway (whether there are DRM systems implemented or not). And people who tend to break the rules, if it is easier or cheaper to obtain the good that way, will download the data from the Internet, rip it, etc, and will find the means to bypass the DRM technologies, if there are such implemented.

In his opinion, DRM systems are bad for the artists as well, because they impose restrictions on everybody and the main criteria for the success of creative work is its availability—this one thing, which is greatly impacted by the DRM systems.

Furthermore, he believes that "moral" and "immoral" in relation to digital data and its copying are relative notions, and the problem more or less comes down to creators getting "enough of a dangling carrot to go on making shows and music and books and paintings."

On balance, he finishes his speech by summoning the boldness of everybody with the words "Sony didn't get permission. Neither should you. Go build the record player that can play everyone's records. Because if you don't do it, someone else will." [24]

4) Richard Stallman: Another of the classical opponents of the DRM technologies, the founder of the Free Software Foundation Richard Stallman, condemns them [25]. He is particularly against Trusted Computing calling it "Treacherous Computing" implying that "companies can 'trust' your computer to obey them instead of you". He believes it enables companies to examine/record/follow your on-/off-line behavior—to tell which software you use, what your listening behavior is, and much more, endangering your privacy or even security. Furthermore, it restricts your freedom by not allowing you to rewrite/develop your software further, or, if you are able to do so, you are not able to run the changed version.

5) Various: And some general wide spread opinions on the DRM technologies are:

According to the Canadian DRM specialist Gord Larose, defenders of the technology argue that "the difference between fair use and piracy is one of HUMAN INTENT, which no foreseeable technology can divine" and that by the current definition of fair use DRM is doomed to fail [26].

It is further pointed out that "DRM is not just copy protection - it is digital *rights management*, after all. If I have acquired a RIGHT to content, as opposed to a physical medium containing the content, then there is the potential for me to get that content anywhere, anytime, in any format required by evolving technologies." [27] Unfortunately, in many of the current implementations with the restrictions imposed (copying limited to a certain number of devices, content bound to a specific piece of hardware, etc.), that is exactly where DRM fails.

Yet some object to DRM from a philosophical point of view. In their opinion art is a collaborative process that builds on the work of others. For digital media, this is referred to as the "rip, mix, burn" culture, certainly hunted by the DRM systems.

And some even defend the opinion that piracy can be viewed as free marketing and is an inevitable part of an optimal business model [5].

B. Advantages and drawbacks of the technologies for the different parties concerned

1) Authors: create the content.

a) Advantages: For sure there is one great advantage of the DRM systems for the content creators—there is (theoretically) no unauthorized use of their intellectual property. Or, as put by the researchers of the INDICARE[9] project - "Content is only accessible by untampered components created by the official system developers, under the conditions of a valid license issued by a bona fide[10] license creator."

b) Drawbacks: The skeptics however see more than one negative impacts of these technologies on the authors:

If the author's works are not that famous and there is not a wide demand for his works, consumers will be rather unwilling to buy something causing them extra problems and imposing extra restrictions to them as digital data locked in by a DRM system. Consequently, not famous/rising content creators fail to distribute content quickly and therefore to gain popularity.

In order to use the DRM technology, the authors must often pay a high cost and the question is "Is it worth it?" The authors become bound to license creators, which can later on influence the distribution of their works.

2) License creators: create the DRM system.

Creating the license and the system to implement it is the task of the license creating companies, so being their job is mainly positive for them.

a) Advantages: On the plus side for the license creators is as well their ability to shape the final product according to their concepts. They can increase income by binding for example advertisements to the content (mainly in the case of videos) or increase user satisfaction by adding "making of" sections.

Often obtaining the digital good is connected to obtaining a special hardware on which you can run your

[9] The acronym INDICARE stands for the **IN**formed **DI**alogue about **C**onsumer **A**cceptability of D**R**M Solutions in **E**urope.

[10] genuine

data. That is why in many cases the license creators make money not only of the sales of the data, but of the sales of the hardware platform as well.

b) Drawbacks: Consequently, a disadvantage for them is the conflict of interests which arises when the digital data selling company and the platform selling company do not coincide. Digital data distributors insist on more control over the distribution of the data and the platform creators care more about the distribution, usability, and compatibility of the platform.

Another possible drawback is, that these companies are constantly driven by the hacker wars to invest in refining and further developing of their technologies.

3) End users: acquire content.

a) Advantages: They can legally download music/videos from proven quality sources without the danger of contaminating their system with viruses.

Consumers can have exactly what they wish—for example a simple track they want without the necessity to buy the whole album.

In contrast to traditional obtaining of creative content (i.e. going to the shop and buying it), the user can download it anywhere at any time.

b) Drawbacks: However, it is clear that DRM, in its current form, has mainly negative impact on the final user. In short, consumers rights are trespassed, since restrictions not imposed by law are enforced.

Precise drawbacks are:

The fact that often digital good is bound to a hardware platform, so in order to take advantage of obtaining the good, you should buy the platform as well. If you change the hardware (for example music player), you should buy most of you tracks again.

You are mostly not able to play the purchased material everywhere and every time you want (on music players by different vendors, in all geographical regions). You are only allowed to a limited amount of use time/ limited amount of copies.

Sometimes the DRM system installs treacherous software on your computer. It may be able to do other things than officially stated or it does not inform you about the installation or how the software can be removed. This can endanger your privacy, property and security (or the security of your system).

Often the system is far too restricting and does not meet the definition of the so called "fair use"[11] If the digital good is bound to your device in some way or another (by identifying you using the number of your CPU, HDD, etc.), it becomes useless if your hardware crashes irrecoverably. In such cases you should pay again for something you have already bought.

DRM systems are mostly clumsy and inflexible towards developments of technology. It is possible that in some future point your data becomes inaccessible, because devices that read the particular formats are not produced anymore or the DRM system is not compatible with the new version of your operating system, etc.

Since, when it comes to music, tracks have to be authenticated to play, they may also become unusable if a download company goes out-of-business.

Additionally, there is always the danger of misuse of personal data—with commercial purpose/ fraud.

Sometimes the companies "reserve their rights to make changes" to the terms of use, so that after a certain period of time you do not even know under what legal conditions you use your software/data/... [5] [28] [29] [19] [11] [2] [30] [10]

4) The society's point of view:

a) Disadvantages for society: Apart from the drawbacks for the private user, specialists point out some socially negative impacts as well:

DRM restricts progress, hindering the development of innovative technologies. On the one hand, it puts "new features under the veto of incumbent industries who fear being out-competed by new market entrants", and on the other hand, repulses the users to try these technologies if they are locked in by a DRM system.

DRM makes long term preservation and archiving difficult, premises essential for preserving cultural identities and diversity of languages.

b) What society does about it: Yet, in many cases, society has recognised many of the possible dangers and has taken measures in order to escape them:

In some countries (with Germany among them) it is required by law from the distribution companies to inform their customers if they are using DRM technologies. Of course, when you are warned about it, you cannot later argue that the product does not meet your expectations.

[11] Yale's definition of fair use: An affirmative defense to copyright infringement set forth in Section 107 of the Copyright Act of 1976 (17 U.S.C. §107) that allows certain persons or entities to use, access, copy, distribute, remix, publicly perform, or publicly display limited portions of protected material for certain purposes. Under the fair use doctrine, such parties may be able to use the protected work without having to receive the copyright owner's permission to use or access that material, or without having to pay the owner for that use or access.

Groups concerned	Positive	Negative
Authors	Less unauthorised use of their intellectual property	Rather unlikely to become famous if they are not already
		High implementation cost
		Bound to a concrete license creator
License creators	Make a living	Conflict of interests if platform and content selling companies do not coincide
	Able to shape the product in accordance to their concept	Constant war with hackers
Consumer	Possible to legally download content	If a digital good is bound to a hardware platform should buy both
	Can get exactly what they want (single tracks rather than buying a whole album)	Limited amount of use time/copies
	Able to download content anywhere at any time	Treacherous software installed on user's computer
		Restricting fair use
		Often has to buy content again if system crashes irrecoverably or is updated
		Privacy endangered
		Terms of use constantly changing
		Content not accessible if company goes off business
Society		Hindering technical progress
		Problems with legacy preservation

TABLE I
Advantages and Disadvantages of DRM for all the parties concerned

Often there are non-governmental organisations which are engaged in the issue and struggle to raise awareness and preserve user's rights. The Electronic Frontier Foundation has scored many victories against user's rights violation, organised protests, etc [31] [8]. The INDICARE Project organises conferences and forums on the topic of DRM, "help to reconcile heterogeneous interests of multiple players" and has issued a Consumer's Guide on the Digital Rights Management [2]. The aim of the Open Rights Group [32] is also raising of awareness, "preserving the civil liberties in the digital world".

c) What can you do: And last, but not least, I take a look at the measures the private user can undertake, when not satisfied with the conditions offered by a DRM technology (apart from bypassing the technology illegally). First and foremost, you should always read the labels of the CDs and DVDs and the terms of use of the software and other digital content you purchase. Unfortunately, that does not save you in cases when the producer "reserves its rights to make changes" to the terms of use [2]. What is more, one cannot enforce his/her rights over unfair use of DRM. One of the few things you can do, when you are not content with the license agreements, is not accepting the terms of use (and consequently not buying the product), making a powerful statement towards the producer that something is wrong.

V. Conclusion

Digital technologies are now constant part of the every day life of millions of people all over the world. That is why it is vital to be informed what your rights, privileges and obligation concerning these technologies are. The current paper has provided a broad overview on the topic. It has been shown that Digital Rights Management technologies surround us at home, at work, in our leisure time. The paper summarises the most common implementations of these technologies and gives a brief input on the most common ways on which they are surmounted. Further, the technical side of the problem is compared to the legal, underlining that copyright protection laws and DRM technologies are different things and that often, the DRM technologies exceed the legal rights and obligations they have been given by law. The paper concludes by overview of the consequences of DRM for authors, license creators and users of digital content drawing the conclusion that they have many disadvantages, primarily for final users, but not only, and suggests that an alternative, user friendly approach to the matter should be found.

References

[1] Webopedia definition of DRM. [Online]. Available: http://www.webopedia.com/TERM/D/DRM.html

[2] M. Groenenboom, D. Helber, D. C. Orwat, D. M. Schaub, and M. Spielkamp, "Consumer's guide to Digital Rights Management," apr 2006, part of the INDICARE Project. [Online]. Available: http://www.indicare.org/tiki-download_file.php?fileId=195

[3] R. Hewison. Lenslok. The Bird Sanctuary. [Online]. Available: http://www.birdsanctuary.co.uk/sanct/s_lenslok.php

[4] (2009) What is iTunes? Apple Inc. [Online]. Available: http://www.apple.com/de/itunes/whatis/

[5] D. Bergemann, T. Eisenbach, J. Feigenbaum, and S. Shenker, "Flexibility as an Instrument in Digital Rights Management," in *Cowles Foundation Discussion Papers*. Cowles Foundation, Yale University, apr 2005, no. 1505. [Online]. Available: http://ideas.repec.org/p/cwl/cwldpp/1505.html

[6] Musicload - Frequently Asked Questions. Deutsche Telekom AG. The website of the German online music store Musicload. [Online]. Available: http://www.musicload.de/

[7] HDMI - Resources - Frequently Asked Questions. HDMI Licensing, LLC. [Online]. Available: http://www.hdmi.org/learningcenter/faq.aspx#1

[8] (2002-2008) The DRM Dictionary. Information Mechanics Ottawa Inc. [Online]. Available: http://www.info-mech.com/drm_dictionary.html

[9] K. Coyle, "The Technology of Rights: Digital Rights Management," nov 2003, lecture, based on a talk originally given at the Library of Congress. [Online]. Available: http://www.kcoyle.net/drm_basics1.html

[10] J. Walker. (2003, sep) The Digital Imprimatur: How big brother and big media can put the Internet genie back in the bottle. Critique towards DRM. [Online]. Available: http://www.fourmilab.ch/documents/digital-imprimatur/

[11] H. Jonker, S. Mauw, J. Verschuren, and A. Schoonen, "Security Aspects of DRM Systems," Eindhoven University of Technology, Department of Mathematics and Computer Science, TNO ITSEF BV, Tech. Rep., 2004. [Online]. Available: http://www.win.tue.nl/~sjouke/publications/papers/security-of-DRM.pdf

[12] D. Isenberg. (1998, jan) Digital Watermarks: New Tools for Copyright Owners and Webmasters. WebReference. [Online]. Available: http://www.webreference.com/content/watermarks/

[13] S. Möller. (2007, sep) Interview mit Raphael Wimmer: Digital Fingerprinting - Eine der wichtigsten Technologien für die Zukunft des Internets. Telemedicus online journal. [Online]. Available: http://www.telemedicus.info/article/422-Interview-Digital-Fingerprinting.html

[14] M. Wu, W. Trappe, Z. J. Wang, and K. R. Liu, "Collision-resistant fingerprinting for multimedia," *IEEE SIGNAL PROCESSING MAGAZINE*, vol. 21, pp. 15–27, mar 2004.

[15] *SWIFTAlliance Access Security Guide for Windows Systems*, 5th ed., S.W.I.F.T., 2004.

[16] (2001, jun) European Copyright Directive. Official Journal L 167. European Parliament. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

[17] (1998, oct) The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary. [Online]. Available: http://www.copyright.gov/legislation/dmca.pdf

[18] (1996, dec) WIPO Copyright Treaty. World Intellectual Property Oraganization. [Online]. Available: http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html

[19] N. Helberger, "Digitales Rechtemanagement und Verbraucherinteressen. Plädoyer für eine DRM-Agenda, die auch die Interessen der Verbraucher berücksichtigt," *Technikfolgenabschätzung: Theorie und Praxis*, vol. 2, pp. 33–40, aug 2006. [Online]. Available: http://www.itas.fzk.de/tatup/062/helb06a.htm

[20] (2007, jun) GNU General Public License, Version 3. Free Software Foundation, Inc. [Online]. Available: http://www.gnu.org/copyleft/gpl.html

[21] Was ist CC? [Online]. Available: http://de.creativecommons.org/was-ist-cc/

[22] C. Farivar. (2006, dec) CE-Oh no he didn't! Part XXI : Gates tells consumers to ditch DRMed tunes, buy CDs. [Online]. Available: http://www.engadget.com/2006/12/14/ce-oh-no-he-didnt-part-xxi-gates-tells-

[23] S. Jobs. (2007, feb) Thoughts on Music. Apple Inc. Steve Jobs on DRM. [Online]. Available: http://www.apple.com/hotnews/thoughtsonmusic/

[24] C. Doctorov. (2004, jun) Microsoft Research DRM talk. [Online]. Available: http://www.craphound.com/msftdrm.txt

[25] R. Stallman. (2006) Opposing Digital Rights Mismanagement. First published by BusinessWeek Online. [Online]. Available: http://www.gnu.org/philosophy/opposing-drm.html

[26] G. Larose. Why DRM sucks? [Online]. Available: http://www.info-mech.com/drm_flaws.html

[27] ——. Why DRM is great! [Online]. Available: http://www.info-mech.com/drm_is_great.html

[28] B. Ballmann. (2003, jul) Digitaler Maulkorb? Kritische Auseinandersetzung mit neuen Technologien und Gesetzen. Chaos Computer Club e.V. [Online]. Available: http://www.ccc.de/digital-rights/

[29] M. Fetscherin, "Stakeholders in Digital Rights Management, The case of music industry," *INDICARE Monitor*, vol. 1, pp. 27–30, jul 2004. [Online]. Available: http://indicare.berlecon.de/tiki-read_article.php?articleId=27

[30] H. Jonker and S. Mauw, "Core Security Requirements of DRM Systems," Eindhoven University of Technology, Department of Mathematics and Computer Science, Tech. Rep., 2005. [Online]. Available: http://alexandria.tue.nl/extra1/wskrap/publichtml/200524.pdf

[31] (2009) Electronic Frontier Foundation. Essence & Campaigns. [Online]. Available: http://www.eff.org/

[32] About Open Rights Group. Overview over the goals and achievements of the Open Rights Group. [Online]. Available: http://www.openrightsgroup.org/about-org/