LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

DRM Circumvention and Criminal Sanctions

Niko Tuononen

Laurea-ammattikorkeakoulu

DRM Circumvention and Criminal Sanctions

Niko Tuononen
Liiketalous
Opinnäytetyö
Kesäkuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Liiketalous
Tradenomi (AMK)
Niko Tuononen

Niko Tuononen

Digitaalisen käyttöoikeuksien hallinnan kiertäminen ja rikosoikeudelliset seuraamukset

Vuosi 2018 Sivumäärä 61

Tämän opinnäytetyön alkuperäinen tarkoitus ja tavoite oli tutkia digitaalisen kopiosuojauksen käyttöä digitaalisissa tuotteissa, kopiosuojauksen purkuun liittyviä sanktioita, sekä kopiosuojauksen kierron mahdollistamista oikeustieteellisten opintojen lopputyönä. Alkuperäistä lopputyötä on sittemmin täydennetty Liiketalouden opintojen kannalta olennaisella sisällöllä. Alkuperäinen lopputyö keskittyi tutkimuskysymysten oikeudelliseen arviointiin, samalla kuitenkin ottaen kantaa epäsuorasti myös aiheeseen yritystoiminnan kannalta. Opinnäytetyö käyttää hyväkseen laadullista tutkimusta, tukeutuen alan kirjallisuuteen ja oikeustapauksiin, samalla kuitenkin ottaen vaikutteita myös ei-tieteellisistä lähteistä.

Opinnäytetyö toteaa, että kopiosuojauksen käytössä on niin oikeudellisesti kuin liiketaloudellisesti paljon muuttujia, jotka on otettava huomioon yritystoiminnassa. Kuluttajien näkökulmasta digitaalisen kopiosuojauksen käyttö voi johtaa jopa täysin toimimattomaan tuotteeseen, josta johtuen yritysten on tehtävä tarpeelliset vertailut ja analyysit pohtiessaan digitaalisen kopiosuojauksen käyttämistä.

Asiasanat: Käyttöoikeuksien hallinta, kopiosuojaus, laki, digitaalinen, IT

Laurea University of Applied Sciences
Degree Programme in
Business Management
Niko Tuononen

Abstract

Niko Tuononen

DRM Circumvention and Criminal Sanctions

Year 2018 Pages 61

The original purpose of this Bachelor's thesis was to research the usage of digital copy protection in digital products, sanctions related to the circumvention of DRM, and the possibility of circumventing DRM as a part of Bachelor of Law studies. The Bachelor's thesis has been subsequently supplemented with content more fitting to a Business Management degree. The original thesis focused on the legal analysis of the research questions while also indirectly considering the topic from a business perspective. The thesis uses a qualitative method with sources from legal literature and cases, while also using non-scientific sources.

The thesis notes, that the usage of DRM has many variables both in legal and business sense, which would need to be taken into consideration in a company. From the perspective of a consumer, the usage of DRM could at its worst lead into a completely unusable product, which means that a company wishing to use DRM should make all the necessary comparisons and analyses when considering the usage of DRM in their digital product.

Keywords: DRM, copy protection, law, digital, IT

Sisällys

1 Introduction

Copyright, or authors' rights as some countries call them, is an undisputable right of the creator. Copyright gives the creator exclusives rights as to how to use and distribute the work, whatever that work may be. Problems arise when these rights are violated, and copyright infringement is punishable by law. If this work is, for example, a physical item such as a book, distributing it would require making physical copies of the book and that in and of itself requires more effort than the average citizen is most likely willing to go through. While copying physical items takes a considerable amount of time and effort, copying and distributing digital goods in comparison is extremely easy. Even before high-speed internet, computers facilitated copying and distributing digital information in a relatively easy manner. A well-known advertisement reminding users "Don't copy that floppy" clearly shows that even before internet was what it is today, copyright infringement and piracy were issues to be tackled. Today, when internet's transfer-speeds have advanced into the realm of gigabits instead of just mere megabits per second, illegal file sharing has become easier than ever.

In recent years' digital goods have risen in popularity and digital content delivery has become increasingly more popular due to its ease of use. In the music business, for example Spotify, Google Play Music and Apple Music all offer their whole catalogue of music for a flat monthly subscription. In movies, different service providers such as Google Play or Apple's iTunes offer digital delivery of films directly into your smart device of choice, be it a smartphone or an Apple TV. The same can be said for books with services such as Amazon's Kindle. Video games have their own digital stores as well, such as Steam, the popular PC game store or Sony's PlayStation Store for its console. No longer is the consumer required to leave the confines of their home to buy a game, a book, or music. The aforementioned ease of copying of digital products and the fact that all these stores sell digital, intangible goods means that the content producers have to have some way of making sure that only those who have actually purchased the product have access to it.

These security measures, or copyright protection measures, are usually referred to as Digital Rights Management or DRM for short. There have been different types of DRM, each of them with a different mechanism of authentication but each of them has had the same goal: making sure that only consumers and users who are authorized to access the product can access it. There have however been problems, as DRM software that has been used before has not been perfect. Tt can be said that DRM has proven to be more bothersome to the legitimate user, rather than those it is actually trying to prevent from accessing the product. There have been cases in which the DRM software used to protect a work, be it a CD or a video game, has been claimed to contain harmful, even malware-like elements or has at some point of the product's lifespan made the product completely unusable by either refusing

to work due to geological restrictions or incompatibility. To these ends, a few class-action lawsuits will be discussed as well as some academic works about DRM to illustrate the issues some DRM software can cause. This is not to say that all DRM that has been used is faulty, in the course of this thesis DRM implementations will be referenced, which have worked better in their intended purpose without inconveniencing the paying user as other DRM solutions have. DRM circumvention is generally considered to be prohibited.

The aim of this thesis is to analyze whether the prohibition of DRM circumvention can include mandatory exceptions for consumers. To this end, the thesis seeks to answer the following research questions: Firstly, what are the sanctions for DRM circumvention and secondly, what can be the exceptions to prohibition of DRM circumvention. This thesis utilizes a qualitative methodology. Sources chosen for this topic have been chosen from a wide variety of legal systems, ranging from Universities from the US to the UK to some case law on the matter.

The sources are primarily related to DRM, while others have as their subject the newly announced Digital Single Market of the EU. Relevant legislation ranging from the international WIPO treaties to national legislation from Finland has been used. DRM has been discussed in the legal world quite a lot in the preceding years, however not much progress has been made, in fact it could be said that things have become increasingly difficult for the paying user, as has been already mentioned above and will be expanded upon below. As such, it is the author's opinion that some sort of discussion should be maintained on the subject, as from a consumer perspective not much positive change has happened when considering DRM as a security measure against copyright infringement.

2 Copyright and consumer rights

Copyright is a right which gives the author of a work certain exclusive rights. The Finnish Copyright Act provides the following:

"(...) copyright shall provide the exclusive right to control a work by reproducing it (...) The reproduction of a work shall comprise making copies of the work in whole or in part, directly or indirectly, temporarily or permanently and by any means or in any form whatsoever.[1]"

Copyright acts dictate what is, and what is not a work that is protected under copyright law, the main definition of such a work being, however a literary or artistic work. Lists describing these types of works are thus by necessity non-exhaustive. Perhaps due to this the Finnish Copyright Act for example simply states that "A person who has created a literary or artistic work shall have copyright therein (…)"[2]. Copyright, then, can subsist in a variety of works. As to exclusions to copyright, the situation is completely opposite. While ideas are something which cannot be copyrighted, the Berne Convention for Protection of Literary and Artistic Works additionally leaves to the countries of the Union to decide whether to offer protection to certain types of works, such as legislative texts[3]. The area of works that can be copyrighted is extremely wide and as long as the work is not anything mentioned in the exclusion list it can be protected by copyright.

The Finnish Copyright Act Chapter 7 is wholly dedicated to penal sanctions and liability in the cases of copyright infringement. While some of the infringements are criminalized and as such punishable under the Finnish Penal Code, the Copyright Act itself contains numerous infringements and offers sanctions for these infringements[4].

Digitalization brought with it issues, which copyright law at that time simply could not cope with. Due to this, amendments regarding technical protection measures and rights management information had to be implemented. Furthermore, a new type of copyrightable form

---

[1] Tekijänoikeuslaki, 404/1961, Ministry of Education, section 2, art 1 and 2.
[2] Ibid, section 1, art 1.
[3] Berne Convention for the Protection of Literary and Artistic Works (1979), article 2 (4).
[4] Ibid. chapter 7.

had to be added, this being the computer program, which is considered to be a literary work. Some of these amendments have been added to the Finnish Copyright Act, after which the previously mentioned Chapter 7 now includes provisions which prohibit circumvention of technological protection measures as well as distribution of devices capable of circumvention.

2.1 Copyright and digital goods

"Goods sold online range from clothes and shoes, to food and houses. The purchase of physical goods (…) is being replaced by the sale of the equivalent digital products without a material carrier over the internet."[5] The main difference between digital and physical goods is indeed in the delivery mechanism. When ordering digital goods, the items themselves are usually delivered through the internet and as such no physical item is transferred, only data. As the main topic of this thesis is Digital Rights Management software, it should however be noted that DRM is employed in some physical goods as well, such as music CD's, movies, or these days more prominently in video games. The reason for this is that these products can be turned into digital files extremely easily, and preventing this was at certain times indeed the entire point of copyright protection. Music, video games and movies are offered in both digital and physical format and the customer can make the choice of purchasing them either through a digital storefront or from a regular retailer or e-tailer and then receive a physical disc with the content on it. In both cases, the content is protected by copyright and generally has some sort of copy protection employed.

For physical goods, excluding previously mentioned products that can be easily turned into digital files, copyright laws were enough for a long time and there was no need for new penalized actions or any sort of drastic changes. For digital goods, this was not the case. This is not to say, that digital goods somehow have made copyright laws completely outdated or useless. The issue with digital goods is that previously there was no similar technology which would be able to provide exact, carbon-copies of products extremely fast. Today digital goods, such as movies, e-books, music and video games are all protected by copyright law. This has not, however, always been the case. Books, movies and music CD's are and were protected by copyright, whether they are in a physical or digital format. Changes concerning these products were not needed. Computer software, such as video games on the other hand did not originally fit to the above definition of copyright and was not indeed even included in

[5] Lima, F. *et al*. The economic dimension of the digital challenge: a copyright perspective, Intellectual Property Quarterly, 1, 2005, p 69.

copyright laws as works which would require protection. The reason for this is fairly simple, computer software as a product is relatively recent and because of this, amendments were needed when its status as a copyrightable work came into question. Computer software at first did not have copyright protection.

In order to remedy this, the World Trade Organization in its TRIPS Agreement article 10 grants computer programs, whether in source or object code, protection as literary works[6]. A year later this addition was mirrored by World Intellectual Property Organization (WIPO), in its Copyright Treaty[7]. With the TRIPS Agreement and the WIPO treaty, computer programs had finally been given the protection of copyright as literary works. In the European Union, the protection of computer programs, including restrictions of acts relating to alteration of a computer program has been separated into its own directive, which is the directive 2009/24/EC on the legal protection of computer programs. As for the protection of technological measures and rights management information in other products in European Union, the directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, commonly known as the InfoSoc Directive, provides protection for these measures by implementing the provisions of both WIPO Copyright Treaty as well as the WIPO Performances and Phonograms Treaty[8]. The United States' way of domestically implementing both of the WIPO Treaties and provide protection to technical protection measures, was to introduce the Digital Millennium Copyright Act (DMCA)[9]. Unlike in the European Union, the DMCA does not make any distinction as to the protection of computer programs. The WIPO Treaties are thus at the heart of both the United States' as well as the European Union's copyright law. While at the beginning computer programs did not have any copyright protection, they do so now and the protection is very much warranted.

As previously stated, the issue of digital goods is that it is very easy to copy and reproduce a perfect copy of them. Furthermore, "[f]rom the viewpoint of authors and owners, (…) the increased ability to copy works, the high quality of digital copies, (…) bear the risk of infringing moral rights as well as economic rights."[10] While physical products of course can be subjected

---

[6] World Trade Organisation, Agreement of Trade-Related Aspects of Intellectual Property Rights (1995), Article 10.
[7] World Intellectual Property Organization, Copyright Treaty, December 20, 1996, art 4.
[8] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001: the harmonisation of certain aspects of copyright and related rights in the information society OJ L167/10, para 15.
[9] Hua, J. Toward a More Balanced Model: The Revision of Anti-Circumvention Rules, Journal of the Copyright Society of the U.S.A. Spring, 2013, p 329-330.
[10] Akester, P. The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture; European Intellectual Property Review, 32 (8), 2010, p 373.

to copyright violations and illegal copying, the process is obviously much more laborious and requires more resources. CD's, movies and video games are in a relatively unique position in that even though one buys a physical product from a brick and mortar store, the digital files can be accessed with a computer and copied off of the CD or DVD and into the computer's hard-drive. Considering this, printed books do not require any form of digital copy protection as there is no easy way for the general consumer to digitize a printed book. Compared to their physical brethren, e-books on the other hand are a completely digital product and as such some form of copy protection would need to be utilized.

Copyright legislation provides for some protection against copyright infringement, however, with digital products normal copyright protection by legal means has not been enough. Due to rampant piracy, copyright owners had to adopt self-help measures, such as previously mentioned DRM solutions and other technological protection measures (TPM) to make sure that the software was only used by legitimate owners. Copyright law is the first layer which protects copyright owners' interests and DRM and TPMs are the second layer. A third layer consisting of anti-circumvention legislation was added by lobbying after copyright owners found out that DRM and TPMs were unsuccessful in protecting their interests.[11] Copyright holders are these days required to supplement the protection given to their works by legislation with these self-help protection measures. These measures are then protected and supplemented by the previously mentioned anti-circumvention laws, which effectively make circumventing copy protection software illegal. The sanctions one gets from circumvention however vary wildly between countries. In the EU, for example, sanctions for circumventing TPMs and DRM range from civil remedies to severe criminal sanctions.[12]

2.2 DRM regulations

While copyright legislation has been around for a long time, legislation concerning and governing DRM has only existed for the last 20 years or so. As mentioned earlier the WIPO treaties were the international treaties which were the push towards the treaties which would govern and protect digital protection measures in the EU and the U.S. Even though the term Digital Rights Management, or DRM, is a term which is used widely today, it does not exist in

[11] Hua J. *supra nota 9*, p 328.
[12] Favale, M. Fine-tuning European copyright law to strike a balance between the rights of owners and users, European Law Review, 33 (5), 2008, p. 693.

any legislation governing it. WIPO Copyright treaty article 11 and 12 mention Technological Measures and Rights Management Information (RMI) respectively. Article 11 discusses the requirement of Contracting Parties to provide adequate legal protection and effective legal remedies against circumvention of technological measures while Article 12 provides that Contracting Parties should provide legal remedies against persons who perform acts that for example remove RMI or distribute works in which RMI has been removed.[13]. No real definition as to what these technological measures mentioned in Article 11 might be is given in the Copyright treaty. Rights Management Information on the other hand is identified in Article 12, subsection 2 as information which for example identifies the work, author or owner of any right in the work.[14]

In the European Union, as mentioned earlier, the Directive 2001/29/EC (InfoSoc directive) implements the same provisions set out in the WIPO Copyright Treaty. Chapter 3 of the Directive concerns the protection of technological protection measures (TPM's) and rights management information. Article 6 within chapter 3 concerns obligations as to technological measures while article 7 deals with obligations concerning rights-management information.[15] Article 6 (1) of the InfoSoc directive contains the prohibition of circumvention of TPM's and as such DRM in general.[16] While the WIPO Copyright treaty provided no definition as to what a technological measure might be, Article 6 (3) of the EU InfoSoc directive provides that technological measures "means any technology, device or component that (…) is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder (…)"[17]. It is furthermore provided that these measures are deemed to be effective when the work is protected through access control or protection process, like encryption or scrambling or any control mechanism which achieves the protection objective[18] As to the rights-management information definition, the EU directive uses the exact same definition as is found in the WIPO Copyright Act.

The European Commission commissioned a study concerning the implementation of the InfoSoc Directive in its Member States from the Queen Mary Intellectual Property Research Institute, which, among others, includes research into the transposing of Article 6 (1) of the Di-

[13] WIPO Copyright Treaty, *supra nota 7*, art. 11, 12.
[14] Ibid, art 12.
[15] Directive 2001/29/EC *supra nota* 8, chapter 3.
[16] Ibid. Article 6 (1).
[17] ibid. article 6, (3).
[18] ibid.

rective. According to the study, most Member States have implemented the Article in chapters dealing with sanctions for copyright infringement, while others have implemented it as an annex to the list of exclusive rights. The study goes on to explain that the first approach could mean that most Member States may not wish to apply the Article to acts which are not restricted acts according to copyright law. Some Member States in the second group furthermore mention that TPM's are a method exclusively used to the right holder while some Member States have opted for a weaker definition by permitting the right holders to use TPM's[19]. The study goes on to discuss and describe different descriptions used in different countries. In Estonia for example, circumvention is described as unlawful use of the work.[20]

The anti-circumvention protection in the European Union is separated into two different directives. The InfoSoc directive article 1, section 2 (a) states that the directive leaves intact and does not affect the legal protection of computer programs.[21] This is relevant because video games are in some cases considered to be computer programs and circumvention in these cases needs to be considered by different rules than when the InfoSoc Directive would be applicable. The World Intellectual Property Organization has conducted some research to determine whether a video game is considered to be a computer program or not. According to them what makes classification a problem is that modern video games contain at least two parts: audiovisual elements and software. Because of these two entirely different elements some jurisdictions consider video games to be predominantly computer programs whereas others give them a distributive classification and finally few countries consider them to be essentially audiovisual works.[22] Computer programs are protected by a specific directive in the EU, which is the directive 2009/24/EC.

While the European Union has been covered by the InfoSoc Directive mentioned previously, the United States' legislation concerning the copyright protection of digital goods should be mentioned. Previously it has already been mentioned that the U.S implemented the provisions set out in the WIPO Copyright Treaty with their Digital Millennium Copyright Act of 1998 (DMCA). The DMCA itself is divided into five titles, out of which the first one implements both of the WIPO Treaties, the Copyright Treaty as well as the Performances and Phonograms Treaty. While the content of the DMCA may mirror the WIPO Treaties, some changes have

---

[19] Westkamp, G. The Implementation of Directive 2001/29/EC in the Member States, Part II, Queen Mary Intellectual Property Research Institute Centre for Commercial Law Studies, 2007, p. 54.
[20] Ibid, p 55.
[21] Directive 2001/29/EC *supra nota* 8, Article 1, section 2(a)
[22] World Intellectual Property Organization, Video Games, http://www.wipo.int/copyright/en/activities/video_games.html (accessed 10.4.2016)

been made. The WIPO Treaties used the wording "Rights Management Information", while the DMCA uses the wording "copyright management information" the definition itself is similar if worded differently. The DMCA defined copyright management information as "identifying information about the work, the author, the copyright owner, and in certain cases, the performer, writer or director of the work, as well as the terms and conditions for use of the work (…)[23]. For the purposes of this thesis, two sections of the DMCA are the most important. Section 1201 includes the prohibition of circumvention of copyright protection systems, while section 1202 deals with previously mentioned copyright management information.

Given that both the DMCA and the InfoSoc Directive use the WIPO Treaties as their basis, the main content of the articles mentioning both RMI and technological measures is relatively similar. As such, it is quite interesting to note that no real requirements or any kind of minimum standards for these technological measures or RMI are given in the legislation. Mainly, what is stated and is a requirement is that Contracting States provide legal remedies and legal protection against circumvention of these measures. The legislation states that protection measures should not be circumvented, and for anyone doing just that a punishment of some kind should be issued. While no real requirements or standards are not given in the legislation, the WIPO Treaties do mention that, for example the technical measures need to be effective. The same requirement for effectiveness is mentioned in the InfoSoc directive Article 6, section 1. No explanation is given as to what an effective measure would be. Considering, that for example in the Video Game industry, circumventing DRM solutions is quite prevalent and not many solutions remain effective for long, the requirement of being effective does seem interesting. The InfoSoc Directive does provide a definition for TPM's but that definition does not itself provide a minimum standard as to what the measure should do and what it should not. It should however be noted, that the anti-circumvention protection is not absolute and as such not all acts of circumvention are violations of article 11 of the WIPO Copyright Treaty. Given this little detail, anti-circumvention measures which prevent acts permitted by law do not require legal protection.[24] Thus some restrictions have been set regarding anti-circumvention measures, while no restrictions, or indeed any type of standards or minimum requirements, have been set for technological protection measures or rights management information.

---

[23] H.R. 2281 — 105th Congress: Digital Millennium Copyright Act, Section 1202 (C).

[24] Akester, P. The impact of digital rights management on freedom of expression - the first empirical assessment, International Review of Intellectual Property and Competition Law, 41 (1), 2010, p 56.

2.3 Technical methods of DRM

DRM as a term does not appear in any of the official legal documents, but is either considered to be a technical protection measure (TPM) or a rights management information (RMI) or some combination thereof. DRM however is a term which has been commonly adopted to mean a technical copyright protection solution in a product which is in digital form. These products usually contain music, movies, video games or eBooks. Besides software, DRM can be found inside hardware, to for example prevent tampering of the device. The main reason for DRM is to restrict unauthorized access, that is, to make sure that only those who have bought the product are able to use it, and to restrict unauthorized copying of the product.

From the copyright holder's point of view, DRM "ensures that content providers - in particular copyright owners - receive adequate remuneration for the creation of the content that is distributed over the DRM system."[25] These, however, are not the only purpose for DRM. Furthermore, DRM "covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets (…)."[26] In addition, DRM can be used to monitor the usage of the product and track the rights. As for authentication, there are a couple of different ways these have been achieved over the years, while currently authentication has become more and more reliant on an active internet connection. This chapter, and this thesis in general focuses on DRM in software form and as such excludes DRM in hardware. This chapter will explain DRM basics and go through different authentication methods which have been used in DRM, as well as the usage of DRM in different industries. The next chapter on the other hand will focus on issues which have been encountered and which have most likely happened due to DRM.

As mentioned earlier, the amount of tasks which DRM systems have to fulfil is relatively large. In the times past, the sole purpose of DRM was to make sure that only those authorized could access the product and to makes sure that no illegal copying could take place. These days it does seem that DRM has in essence been integrated into many online marketplaces. What this essentially means is that content which is purchased from the webstore is locked to the user account and this lock essentially functions as DRM. Whether a DRM solution is used or not, the

---

[25] Bechtold, S., Digital Rights Management in the United States and Europe, American Journal of Comparative Law, Spring 2004, p 323 and 324.
[26] Iannella. R., Digital Rights Management (DRM) Architectures, D-Lib Magazine, volume 7 number 6, June 2001.

baseline for protection is always Copyright law, DRM is merely a self-help measure which supplements the protection provided by Copyright Law. There are quite a few different types of DRM which are used, however two of the most used methods are offline key-based authentication and phone-home authentication.[27] Offline key-based authentication usually relied on an alphanumeric key, which would be required to use the product. What is significant for this approach is the fact that no internet connection is required. For video games, this usually meant a slip of paper with a code within the case containing the CD or DVD. This code then would need to be input during the installation procedure to prove that the copy was indeed genuinely bought. The simplest way for this type of authentication method to work is for the system to compare the provided key to a list of acceptable values on the disc itself and then either accept or reject the access attempt.[28]

The issue with the offline approach is that there is no real way to make sure that the key is used only once as no type of online component is used in this authentication type. The same key can be used multiple times, and if the list of acceptable values is somehow discovered, creation of fraudulent keys could be possible. To remedy this, a so-called phone-home authentication method was invented, in which the key was still needed, but instead of a list on the media itself, it would be compared to a list on a central authentication server which would then grant or deny access. The key, which the user provides will be compared by the central server or authority to verify that the key itself is valid and that the key and privileges assigned to it are not already used elsewhere.[29] The main difference between the phone-home and offline key-based authentication is that in phone-home authentication the central server acts as the authentication point and as such can distinguish when a key has already been used and then can reject multiple uses of the same key unlike the offline key-based system. The authentication itself can be only done once, such as in the case of Microsoft Office installation or for example upon each use to make sure that the license has not lapsed.[30]

While usually the phone-home authentication does require an internet connection, the connection does not necessarily have to be continuous. As such, the connection would only need to be used for the authentication itself after which the product could be used without an internet connection. Internet connection itself has become fairly widespread and as such more people have had access to it. With this in mind, a new type of authentication method has

---

[27] Dubbelde. J., A potentially Fatal Cure: Does Digital Rights Management Ensure Balanced Protection of Property Rights, University of Illinois Journal of Law, Technology and Policy, Fall 2010, p 413.
[28] Ibid, p 414.
[29] Ibid, p 415.
[30] Ibid.

gained more traction. Usually dubbed as "Always-online DRM", this type of DRM, as the name implies, requires a constant connection to the internet to work. While the phone-home authentication would need an internet connection only momentarily, an always-online DRM solution requires a stable and constant internet connection to work. This would then mean that the product would essentially become useless without a proper internet connection. Some products use Always-online DRM justifiably, as they indeed do require an internet connection anyway, whether the authentication would be required or not. An example of these kinds of products would be certain video games or streaming services, which rely on an internet connection to supply the content. Other times, the content itself does not require an internet connection, in which cases the connection is only used for authentication purposes.

At least previously, the aforementioned three types of DRM solutions are mainly found on computer software and even more specifically video games. These days the music industry has shifted to a streaming style-distribution, such as Spotify or other such services, where the music is locked to an account and generally cannot be listened to without the account details and as such authentication. The film industry as well uses streaming services, where the purchase is locked to an account. In some cases, physical editions of a film may include a one-time code, which can be used to gain access to a digital edition of the film, which can then be streamed. This key would then authenticate the copy and as such act as a type of DRM check. Music industry, on the other hand used to previously bundle its digital products with a type of DRM. This would, in some cases, show itself as a limitation on how many times the song could be downloaded from the servers, and even in some cases how many times the song could be transferred to a different device, such as an MP3 player. A research, which was done in 2003 revealed that the music industry seemed to use the most protection technologies out of the three industries which were questioned. These industries were the music, film and print industry. The music industry at the time used payment systems, copy detection systems, digital signatures and fingerprints, watermarking, encryption and passwords.[31] The film industry on the other hand solely resorted to payment systems, encryption and passwords, while the print industry only partially protected their digital content with payment systems, watermarking, encryption and passwords.[32] Out of these protection methods, most likely watermarking and fingerprinting are not the most self-explanatory. Watermarking means the embedding of hidden data, such as copyright information within the digital content itself, which

[31] Fetscherin, M., *et al.* Comparing the Usage of Digital Rights Management Systems in the Music, Film, and Print Industry, ICEC '03 Proceedings of the 5th international conference on Electronic commerce, 2003, p 320.
[32] Ibid.

inevitably changes the content.[33] Fingerprinting on the other hand is used for content identification, with the objective to establish equality of multimedia objects by comparing the associated fingerprints.[34] From 2003, companies' interest in protecting their digital content has most likely changed, as for example e-books have grown in popularity and digital content in general has become more prevalent.

As was mentioned earlier, one goal for DRM is that the copyright holders get remuneration for their efforts. As such, there are some cases, where the DRM has not been as noticeable as a code-slip or some such which would need to be inserted to access the product. This type of DRM could be called in-game DRM, as it is more prevalent, and quite possibly a completely unique phenomenon relating to video games. The main reason for this type of DRM is mainly due to the fact that "intrusive DRM may evoke spirited opposition from game players and game reviewers."[35] To combat this issue, endogenous DRM has at time been employed instead of more traditional methods, which have been described above. The idea behind endogenous DRM is that it uses in-game elements which degrade the experience for those players who run an unlicensed copy. The developers may for example shift game mechanics which would cause the game to be buggy or introduce enemies which would be impossible for the player to defeat.[36]

When compared with normal DRM methods, endogenous DRM itself is fairly ingenuous. DRM itself has been mainly considered to be bothersome and furthermore, is usually seen as only inconveniencing the legitimate buyer, when the person who gets a copy illegitimately does not have to bother with intrusive DRM solutions. With endogenous DRM the whole approach to authentication and copy protection itself is different. Implementing endogenous DRM has been met with mixed success. This type of DRM is usually most successful when it is used to frustrate and embarrass pirates, which is usually achieved by introducing some type of obstacles that are very obviously out of place. These obstacles may for example serve to make the game impossible to play or extremely difficult.[37]

---

[33] Jonker, W., *et al*., Digital Rights Management in Consumer Electronics Products, IEEE Signal Processing Magazine, March 2004, p 85.
[34] Ibid. p 86.
[35] Moshirnia, A., Giant Pink Scorpions: Fighting Piracy with Novel Digital Rights Management Technology, DePaul Journal of Art, Technology & Intellectual Property Law, Fall 2012, p 49.
[36] Ibid. p 49-50.
[37] Ibid. p 50.

This type of DRM could easily be considered a revolutionary approach, as it turns the general idea about DRM on its head. While the same result will be achieved both with regular DRM solutions as well as endogenous DRM, the latter does not really inconvenience the legitimate user while the former can very much do that. As such, the endogenous DRM as a copyright protection system, is an example of an approach which, if done properly, is entirely acceptable. The general problem with DRM, as will be more thoroughly explained in later chapters, is that the problems which can arise from an improper implementation or too intrusive DRM solution, can make the product completely unusable in some situations or in some cases even install software on the computer which can be considered malware.

Geo-blocking, which at first glance may not seem like a DRM solution can be defined as "the limiting the user's access to digital content, by the content distributor, based on the user's geographical location. The content is almost always copyrighted, and can be of many natures, whether a television show, song or music album, even a video game."[38] The fact that geo-blocking effectively limits the content to a certain geographical location does make it essentially DRM. Geo-blocking, however, by design does not offer limitations of copying, which generally is associated with DRM. It does, still, fall within the second generation of DRM, which places limitations on the access to content.[39] One very well-known service, which utilizes geo-blocking is Netflix, as the website's film and TV-show offering clearly changes depending on from where the service is accessed.

The overly zealous usage of DRM and the general public's growing distrust of it has reached such proportions that some e-tailers and internet webstores, which mainly deal in video games, have decided to sell their products completely DRM-free. With this approach, the consumer has complete control over where and how he consumes his media and as no authentication is made and as such no DRM is present in the product. While DRM-free products have perhaps centered around the video-game industry slightly more than others, there are exceptions. In the music industry something similar has been attempted previously, although on a smaller scale. In 2007, the band Radiohead released its album "In Rainbows" exclusively through its website, DRM-free, the idea being that the fans were able to set their own price with an option to pay nothing for the album.[40]

---

[38] Kra-Oz, T., Geoblocking and the Legality of Circumvention, Hebrew University of Jerusalem Legal Research Paper No. 15-31, 2014, p 2.
[39] Ibid, p 4.
[40] Moshirnia, *supra nota* 35, p 40

Radiohead's venture into the realm of DRM-free distribution as well as a voluntary pricing model did not end fruitfully in terms of remuneration, as the average price paid for the whole album was $2.26. This price included those who decided to not pay anything for the album.[41] Another example of a voluntary pricing model, and consequently DRM-free approach, comes from the video game industry, the Humble Bundle. The Humble Bundle offers, for a limited time, licensed, DRM-free bundles of independently published video games. These video games are offered on a pay what you want basis, with a minimum one cent licensing fee.[42] The Humble Bundles have continued after the first bundle, which was a success, as it resulted in gross sales which exceeded a goal set to $1 million.[43] Another digital storefront dedicated to DRM-free products is GoG.com, which by their own words "is a digital distribution platform serving fantastic computer games and movies"[44]. They believe that DRM-free world would be a better place, which is why their products come entirely without DRMs or any other intrusive copy protection.[45]

All of these examples serve to explain and illustrate the different ways in which DRM has been used in the past, and that for some, not using DRM is a selling point. The fact that "DRM-free" is a selling point to some, would indicate that these people have adverse feelings towards DRM and its inclusion into products. The next chapter is more focused on the problems which have been found to be connected to DRM in some form or another, and they should at least to some extent shed light into why some people feel that DRM is more of a curse-word rather than the saving grace against piracy which it seems to be to some. To reiterate, however, some implementations of DRM are slightly more unorthodox, as was mentioned earlier and these implementations might not fall into the same category as those which provide more issues. As such, not all DRM is bad or considered to be harmful or annoying to the end user.

2.4 DRM and consumer rights

[41] Ibid. p 41.
[42] Ibid.
[43] Ibid.
[44] https://www.gog.com/support/website_help/what_is_gog_com (accessed 18.3.2016)
[45] Ibid.

This chapter's main goal is to illustrate different issues which have manifested mostly due to DRM, but at the same time have not been severe enough to result in a judicial proceeding. A later chapter will introduce three different cases in which the issues mentioned are due to the DRM solution being used. This subchapter, on the other hand will illustrate different issues, but does not do so via court cases. Instead, this subchapter relies on hypothetical situations or news articles about issues with DRM. The problems listed here are not definitive or exhaustive, but they should give a good enough view on how the common consumer might see DRM and how DRM can hinder the user and experiencing the product.

Geo-blocking as a concept and form of DRM was already mentioned and discussed previously. One of the earliest forms of geo-blocking could be said to be hardware-based DVD region codes. The problem with region coding is of course that for example Europeans visiting United States could not play any DVD's they bought during their trip back home without an American DVD player.[46] Region coding is these days still used, but to a lesser degree. Blu-ray disks implement only a three region system, whereas the DVD had six different regions. Furthermore, however usually Blu-ray releases are un-encoded.[47] The problems of region coding should be fairly easy to see. While the idea of region coding certain releases from a business standpoint does make sense, the idea that a consumer would need to buy a new DVD player to play any DVD's he or she may have bought from another country does not seem fair. Perhaps due to this exactly, region coding itself has been largely forgotten. Geo-blocking itself has not however been forgotten. These days geo-blocking is used, for example, in streaming services such as Netflix or Spotify. The difference with this implementation and region coding is that geo-blocking these days might produce different results for services like Netflix. A consumer traveling to another country could encounter different content, due to the differences between how the service is offered in other countries or actually accessing the service could be impossible due to geo-blocking.[48] From a user's standpoint this type of differentiation of content or even not being able to access it at all due to a different geographical location is a problem in and of itself. Having paid to access some content and then finding out that they cannot access it because they are on vacation in another country could potentially drive the customer to try circumvention methods to access the content they expected to be able to.

---

[46] Kra-Oz, supra *nota* 38, p 7.
[47] Ibid.
[48] Ibid, p 12.

The inclusion of always-online DRM into video games has caused many issues for consumers. Two different video games will be referenced here, which have been released in the last 5 years and have had always-online DRM attached to them. First of these, Diablo 3 was released in 2012 and developed by Blizzard Entertainment. Due to the fact that the product was attached to a DRM solution which required constant communication with the game servers, the game's launch was plagued by connectivity issues. These issues led to a situation in which a French consumer standards organization, UFC Que Choisir received over 1500 complaints over the course of 4 days from gamers about the connectivity issues of the game.[49] The same product came under scrutiny in Germany as well, although this time the issue was that the product packaging did not contain information about the always-online requirement. As such, the Federation of German Consumer Organisations held Blizzard, the developer of the video game account able for antitrust violations. The requirement of always-online DRM as well as tying the game to an account effectively prevented resale, which was another thing which was supposed to be mentioned on the packaging.[50] Another video game released in the recent years to come under fire due to its inclusion of always-online DRM was SimCity, which was released in 2013 and published by Electronic Arts. The game itself suffered from the same type of connection problems as the previously mentioned Diablo 3. The connection issues resulted in delays to access the game, which meant that the game was usually inaccessible due to these issues. The issues were considered so severe, that the publisher decided to disable some of the non-critical features and later on would disable a high-speed cheetah mode of the game.[51]

Finally, an issue which seems to fairly inherent to the usage of DRM: incompatibility. DRM systems are, perhaps by design, not compatible with each other. Some systems lock the content to specific devices, while others to specific software. An example of this would be Apple and its iTunes music service, which originally came with DRM which restricted playing the music to the iPod only.[52] Another example of incompatibility relating to DRM comes from the author's own experience. A video game, which used the StarForce DRM mentioned earlier failed to even start after an upgrade to a newer computer operating system.

---

[49] William Usher, Blizzard Faces Legal Indictments From France, Germany Over Diablo 3, http://www.cinemablend.com/games/Blizzard-Faces-Legal-Indictments-From-France-Germany-Over-Diablo-3-43626.html (accessed 8.4.2016).
[50] Ibid.
[51] Nathan Ingraham, EA disabling 'non-critical' features and adding more servers to address ongoing 'SimCity' connection issues, http://www.theverge.com/2013/3/7/4074878/ea-deploying-more-simcity-servers-to-stem-persistent-connection (accessed 9.4.2016).
[52] Stormdale, C., The problems with DRM, Entertainment Law Review, 17(1) 2006, p 3.

Later on, the same video game was released without StarForce DRM, and worked on the upgraded operating system. As such, conclusions could be drawn that the main culprit for this incompatibility was indeed the DRM system.

These issues, which have been discussed above may seem minimal, however when it is taken into consideration that some of these problems are not only a nuisance, but possibly could ruin the consumer's experience be it for only a limited time or not or even completely make the product unusable, the severity of the problems should be fairly evident. As for the issues which geo-blocking has posed, while not necessarily completely debilitating, they are still issues which the consumer may not be aware of and appreciate. When buying a product, the consumer in good faith assumes that he should be able to view, listen, play or operate the product even while visiting another geographical area. Apparently, at least in the European Union, there is talk about a digital single market which potentially could bring an end to geo-blocking, and as such these problems could be a thing of the past. The digital single market will be discussed more near the end of the thesis.

3 Sanctions for DRM circumvention

The last chapter illustrated the legislations which, at least to some extent, deal with DRM in the European Union and U.S. as well as the WIPO treaties which form the basis for both the InfoSoc Directive in the European Union and the Digital Millennium Copyright Act in the United States. Both the WIPO treaties and the InfoSoc directive leave the sanctions up to the member states to decide. As such, the next section of this thesis focuses on the sanctions and how they differ between EU Member States. The sanctions for circumvention in the United States are discussed as well. Finally, discussion will turn to whether these sanctions are effective using cost-benefit analysis. The unmistakable fact is, that sanctions and fines which are often sentenced for circumvention and over all distributing content illegally be it via peer-to-peer networks or otherwise, can be fairly high. The situation requires looking into, especially when the one who has to pay the ridiculously high fine is your average consumer. There are no excuses as to the fact that the person has committed a copyright infringement, however when the fine turns out to be several thousands of whatever is the applicable currency, and the item in question which was pirated is a movie or a couple of CD's, the fine itself is quite high. Time will be spent discussing whether the high fines and even penal sanctions actually serve a real purpose and if they are enough or indeed, too much, to deter illegal behavior.

3.1 EU InfoSoc Directive

As has been previously seen, the legislation which does, at least to some effect, deal with DRM protection software mainly focuses on preventing the circumvention of these protection systems. What is interesting is that neither the WIPO treaties or the European Union's InfoSoc directive do not define any sort of legal remedies but instead leave it for the contracting parties to decide what type of sanctions and legal remedies are available for circumvention. The only requirement being that these remedies and protection is adequate and/or effective. While the WIPO Treaties stay relatively silent on the sanctions and remedies, the InfoSoc Directive goes slightly further and says the following in its Article 8 on the sanctions and remedies as well as some requirements they should at least fulfill:

"Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary

to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive."[53]

All the requirements are left fairly vague, which is how it should be, as now the Member States have some leeway as to how to approach the sanctions, as the only requirement is that the sanctions and remedies are appropriate. Considering this vagueness, different Member States obviously may have a different view as to what these sanctions should be and what is a sufficient punishment for the crime of circumvention, or indeed whether circumvention should be criminalized at all. Whether it is due to this vagueness or not, the study which the European Commission commissioned from the Queen Mary Intellectual Property Research Institute touches on sanctions. Among the information gathered and analyzed, was indeed what sanctions different Member States impose on the act of circumvention. While the amount of sanctions can vary largely between jurisdictions, the range of them is limited to two general groups: Civil sanctions and penal sanctions.

Some countries even chose to not criminalize the act of circumvention, albeit these countries were in a very small minority. These countries, which chose to intentionally exclude criminal sanctions were the Netherlands, Estonia and Slovakia.[54] Thus, in these countries civil sanctions remain the only option for recourse if someone chooses to circumvent DRM. Some countries on the other hand apply general copyright sanctions, in which case penal sanctions are applied in cases where the infringement is committed in connection with running a business or on a commercial scale. Countries which are using this system are Austria, Belgium, Denmark, Estonia, Greece, Hungary, Latvia, Lithuania, Luxembourg, Norway, Slovakia and Slovenia.[55] Estonia is in both of these lists, which could mean that generally no criminal sanctions are applied, however if the act of circumvention is carried out in a business setting, with the goal to make a profit then criminal sanctions could apply. Some countries provide specific criminal sanctions for acts of circumvention, which are sometimes provided under Penal Law. These countries are Finland, France, Ireland, Italy, Portugal, Spain and the UK. As a side note, Finland and Norway furthermore have a distinction between smaller and more serious offences.[56]

---

[53] Directive 2001/29/EC *supra nota* 8, Article 8, section 1.
[54] Westkamp, G. supra *nota* 19, p. 75.
[55] Ibid.
[56] Ibid.

As the study shows, specific penal sanctions and general copyright sanctions, which may lead to penal sanctions, are in the majority when Member States were deciding on sanctions for acts of circumvention. A small minority did, however, decide to completely exclude penal sanctions. In these cases, civil sanctions are still applicable, so the exclusion of penal sanctions does not mean the total absence of sanctions. With the study's results in mind, it is safe to say that in Europe, with a few exceptions, if one commits the act of circumvention, especially in a business setting for profit, penal sanctions will be applied without much hesitation. It is entirely understandable that penal sanctions are applied in cases where the circumvention happens in a business setting with the goal of making a profit. An issue with these sanctions rises when a regular consumer faces penal sanctions, or high civil sanctions for that matter, for circumventing copy protection solutions.

3.2 The U.S. Digital Millennium Copyright Act

The United States' way of implementing the WIPO Copyright Treaty as well as the WIPO Performances and Phonograms Treaty came in the form of the Digital Millennium Copyright Act (DMCA). While in the European Union, the sanctions were left up to the Member States to decide, the DMCA instead sets numerous sanctions ranging from civil remedies to criminal penalties. Section 1203 of the DMCA empowers the court to grant both monetary and equitable remedies, such as those which are available under the Copyright Act, the remedies furthermore include statutory remedies. Should the violator prove to be innocent, the court has the possibility to reduce or remit damages.[57] As to what is needed for the violator to be proven innocent, the DMCA provides that the court has to find that the violator was not aware and had no reason to believe that the acts themselves constituted a violation.[58] The idea here is of course, that the person would need to not be aware that what he or she was doing was actually illegal.

The DMCA includes provisions for criminal penalties. For these penalties to be applied, the offence has to violate sections 1201 and 1202 willfully and for purposes of commercial advantage or private financial gain.[59] The requirements for Criminal Penalties to apply are fairly

---

[57] Becker, E. et al, Digital Rights Management, Technological, Economic, Legal and Political Aspects, Germany, Springer, 2003 p 371.
[58] Digital Millennium Copyright Act, *supra nota 21,* Section 1203 (c) (5) (A).
[59] Becker, *supra nota* 57.

similar to those of the countries in European Union which applied general copyright sanctions. The act of willfulness was not mentioned in the requirements in European Union, however one would presume that it is implicit. As such, the requirements for criminal sanctions seem to be relatively the same in both the United States as well as countries in the European Union which apply general copyright sanctions. In addition to the requirements which would need to be fulfilled for criminal penalties to apply, the DMCA further goes on to specify penalties for these offences. For the first offence, a fine of up to 500.000 USD or up to five years of imprisonment, while for subsequent offences the fine goes up to 1.000.000 USD or up to 10 years of imprisonment.[60] Whether the offence is circumventing copyright protection systems or removing or altering copyright management information, harsh punishments can be nonetheless granted.

With these criminal penalties in mind, it is quite interesting to note that the circumvention prohibition which can be found in 1201 (a) (1) of the DMCA is much broader than the one in Art. 11 of the WIPO Copyright Treaty. The DMCA circumvention prohibition additionally prevents circumvention which are performed for lawful purposes, while the WIPO treaty only requires legal remedies against acts which are not authorized by the rights holders.[61]

3.3 Cost-benefit of sanctions

Sanctions related to digital products' copyright infringement, be it general piracy or otherwise, are generally associated to be fairly high. Even though the main focus of this thesis is Digital Rights Management, software piracy is fairly well intertwined into the topic. Some examples of sanctions which have been issued may not directly deal with DRM circumvention, but rather sharing copyrighted material without the consent of the copyright holder. In these cases, DRM circumvention may still be an element, as for example video games or music shared through different methods usually lack the DRM which is found on the legitimate product. Which is to say that DRM circumvention has occurred at some point. Some companies these days seem to have opted for contacting infringers directly and requesting compensation. This saves the copyright holder Court expenses if the person receiving the letter pays the demanded price. The main reason for these kinds of letters is to avoid court proceedings,

[60] Ibid.
[61] Ibid, p 377.

however obviously if the person does not pay, court proceedings would need to be initiated. While this kind of procedure does not obviously fall within the sanctions and remedies described in any of the treaties mentioned above, the amounts demanded do give some sort of an idea as to what could be demanded from an infringer in court. These sorts of piracy letters have been sent to alleged pirates at least in the UK, the U.S. and Finland. Usually the main idea of these letters is to scare the receiver into paying the fine, however at least in Finland the letters may lead into an actual court case.

In the United States, the sums demanded are "usually between $1000 and $3000"[62], while in the United Kingdom the "[t]ypical sums demanded are in the range of £500 to £1000"[63] In the cases of these two countries, the letters seem to be from companies that do not actually have any desire to go to court, but instead are trying to scare people into paying. The situation seems to be slightly different in Finland. A local law office, Turre Legal, has provided an easy-to-use negotiation service through them, which attempts to lower the sum owed, which depends on the amount of copyright infringements. One infringement results in a 600 € claim while more could result to up to 3000 € demand. According to them, October 2015 saw the start of the first court cases which were started due to these letters.[64] As for actual court proceedings, regarding piracy and DRM circumvention by proxy, a fairly high-profile case in Finland, which even went as far as the Supreme Court of Finland was a case regarding a popular Finnish torrent website Finreactor. The administrators of the website ended up appealing all the way up to the Supreme Court, where the amount of fines they had to pay actually went up, all the way to 680 000 €. The case had 11 defendants in total, and as such the amount to be paid was divided between them. The defendants were in addition found guilty of copyright infringement which resulted in a penal sanction.[65]

Here we can clearly see that the sanctions for copyright infringement, at least in Finland, can be extremely high. The problem here is of course, that usually the persons who are found guilty in cases of copyright infringement which is essentially piracy or circumvention of copyright protection measures are normal people who might not have thousands to spare. Thankfully in the case mentioned above, the amount was divided between 11 persons. Regardless, not that many people can afford a sudden charge of almost 70 000 €. As such it requires considerable effort from a regular person to be able to pay the fines. Given that criminal and

---

[62] http://www.pcworld.com/article/230515/So_Youre_Being_Sued_for_Piracy.html (accessed 29.2.2016)
[63] https://torrentfreak.com/received-a-piracy-letter-uk-solicitor-will-defend-you-for-free-150320/ (accessed 29.2.2016)
[64] http://www.turre.com/turre-neuvottelija/ (accessed 29.2.2016)
[65] The Finnish Supreme Court, KKO:2010:47

tort law are directed at deterring costly behavior and as such the benefits of these laws are the crimes and accidents that have been avoided[66] it makes sense that the sanctions and fines would be quite high to deter others, and indeed the defendants themselves, from committing a crime in the future. Another aspect which backs up the quite high damages is the fact that for individuals who use the internet is the probability of actually getting caught for occasionally uploading a copyrighted piece of software is essentially zero.[67] The reason why this is relevant is that because the detection of these types of copyright infringements are so difficult to detect and punish, increasing the amount of the punishment could preserve the level of deterrence[68]. It then could be said that because of the low detection rate, those who are actually caught are made an example for those who are not caught. Whether this actually works is debatable.

The problem with very high damages awarded becomes quite obvious with the following example: "If a potential infringer is unable to pay $2,000,000 worth of damages, there is nothing deterring him from causing $3,000,000 worth of harm."[69] This example becomes even more fitting, when it is realized that today infringing on copyright is extremely easy, as even a college student is able to infringe thousands, or even possibly thousands of dollars' worth of copyright and as such the probability that such a student has the necessary resources to compensate the copyright owners is extremely low[70]. Granted, it would seem that the amount of damages awarded seem to be slightly larger in the United States, than in Finland at least according to the study referenced, however, the main idea still stands. What does indeed prevent a person from doing even more harm if they know that they would have to pay exponentially more than they are themselves worth? Monetary punishment is not the only punishment possibility when discussing criminal sanctions. Incarceration is possibly the ultimate form of criminal punishment, at least in countries where the death sentence is illegal. The problem of imprisonment is the cost, which is extremely high. As we saw in the chapter concerning sanctions in the United States, imprisonment is a real option, mostly in cases where the circumvention is done for monetary gain, but an option none the less.

Criminal sanctions do of course have benefits and they can be more beneficial in deterring crimes. Criminal sanctions are especially useful when self-help measures prove to be costly

---

[66] Buccafusco, C. *et al*. Innovation and incarceration: An economic analysis of criminal intellectual property law, Southern California Law Review, January 2014, p 284.
[67] Hardy, T. Criminal Copyright Infringement, William & Mary Bill of Rights Journal, December 2002, p. 313.
[68] Ibid.
[69] Buccafusco, *supra nota* 66, p 307.
[70] Ibid, p 306.

and civil remedies are not enough to deter the behavior. Still, criminal sanctions should only be adopted if the deterrence benefits actually exceed the cost of the use of criminal sanctions.[71] While the detection rate of copyright infringements committed in the internet is very low, and at first it does look like the deterrence effect of whatever sanctions are set up is extremely low, the desired level of deterrence can still be brought up by increasing the punishment for those who eventually do get caught.[72] The problem with this of course is that if imprisonment is used as a punishment and the times of imprisonment are increased due to this, the cost of the punishment itself goes up exponentially, which once again brings up the question of whether the cost is actually higher than the benefit itself. As an alternative to incarceration however, some other sanctions can be used to create the desired level of deterrence with less cost. These types of alternative sanctions could be "(…) prohibitions on the ownership or use of technologies that are capable of violating copyrights."[73] This would essentially mean that a person would be prohibited from using any type of electronic device which could be used to violate copyrights. When comparing such a sanction to a prison sentence, the advantages do come clear fairly quickly. The infringer could still live home and perform relatively normally within a society and would not be in prison, where his upkeep would be in the hands of the Government. While the deterrent effect of these kinds of sanctions are important, something more important is the incapacitation which these sanctions provide, as these types of sanctions are enforced they would be quite effective in prohibiting the infringers from engaging in future copyright infringement.[74]

While the upsides of criminal sanctions described above can be quite attractive, the sanctions themselves are not without downsides. One of the downsides is the already mentioned cost attached to the sanctions. The costs themselves come from mainly four different actions, which are detection, enforcement, prosecution and sanction, out of these the costs of detection and prosecution of those committing copyright infringement are shared by the public and organizations which represent victims of infringement.[75] Of course these costs are somewhat lessened if instead of incarceration some alternative method is used, such as the prohibition of using technological devices. These days, however, one has to wonder whether the umbrella prohibition is perhaps too restrictive, as some have even discussed adding basic internet connectivity as a basic human right. Granted, it could be extremely difficult to detect when any technological device is used for something illegal and when it is not, and as such a blanket

---

[71] Ibid, p 309-310.
[72] Hardy *supra nota* 67, p 314.
[73] Buccafusco, *supra nota* 66, p 310.
[74] Ibid.
[75] Ibid, p 312.

prohibition for a limited amount of time would be the easiest and less taxing option. Furthermore, the world is extremely digital these days as almost everything can be done on the internet and some banks for example, are making customers pay if they want to get something done in an office instead of doing it online. Cutting someone completely out of the digital life could be seen as a social death sentence, as everything happens on the internet or on the phone and for someone without any way to access these legally it could be a very difficult time. Another quite interesting downside is the idea that while the main goal of criminal enforcement is to deter infringing activity, in doing so it may deter lawful and socially valuable conduct. In connection to copyright infringement, this could mean that the threat of criminal sanctions such as going to jail could prevent a person from using copyrighted material for legal purposes when the usage could in fact be beneficial.[76] This is a fairly interesting point which does bear some truth to it. When considering whether using some type of material in some work or other, the common user most likely errs on the side of caution and as such may choose to decide against using, for example a video clip for fear of it being copyrighted and as such receiving harsh monetary sanctions or even jail time for using it illegally, when in fact it using it was not illegal at all. If this were the case, it could and most likely does in some parts, severely hinder creativity and socially valuable copying. From the point of DRM, one of the probably most important goals of sanctions overall and as such deterrence, is the reduction in socially wasteful self-help measures, among these DRM itself. The main idea behind this is that if the sanctions would lead to improved deterrence, copyright holders would not need to utilize DRM to prevent infringement.[77] Of course whether this would actually be the case is something that is not at all certain. As such, harsh criminal sanctions themselves do not necessarily ease the situation of badly designed DRM at all. One final cost of criminal sanctions comes in the form of public perception. The main idea behind this is that people do not necessarily believe copyright infringement to be harmful and as such subjecting offenders to imprisonment is seen as too much.[78] The perception that copyright infringement is not seen as harmless and the harsh punishments themselves create an interesting gap between public perception and law. In this case, if people think that criminal sanctions are inappropriate for copyright infringement, the deterrence effect of the sanctions themselves is weaker.[79]

As has been seen here, both civil- and criminal sanctions have their own upsides and downsides. Civil sanctions might be seen as more appropriate by the general populace; however,

---

[76] Moohr, G., Defining overcriminalization through cost-benefit analysis: The example of criminal copyright law, American University Law Review, February 2005, p 804.
[77] Buccafusco *supra nota* 66, p 313.
[78] Ibid.
[79] Ibid.

they clearly alone are not enough to deter copyright infringements. Criminal sanctions on the other hand might be able to deter infringing behavior better, but at the same time the costs they bear are significantly higher and the sanctions themselves might not line up with public perception. Still, when considering the benefits and costs of criminal sanctions, the deterrent effect is quite limited, and at the same time the costs to copyright policy itself and to the long-term effectiveness of criminal law may be quite large.[80] From the point of DRM, the main reason for the usage of these self-help measures is the simple reason that sanctions are not enough to deter copyright infringements. It is still doubtful whether the usage of DRM would stop in the hypothetical scenario where deterrence would be high enough. The creation and use of DRM is relatively cheap and using DRM enables copyright holders to protect their works beyond what would normally be possible with just copyright as well as content that itself is not subject to copyright law.[81] Given that DRM is just a self-help method of copyright owners, and that it, while being protected by copyright law, can be applied to content that is itself not protected by copyright law, could easily mean that companies utilizing DRM are not very inclined to discontinue its use.

It has now been established that civil sanctions by themselves do not necessarily offer good enough deterrence effect, while criminal sanctions have their own problems not the least of which is the fact that general populace does not believe them to be necessary. However, given that copyright infringement in general is illegal and circumvention of technological protection measures is illegal and in some cases even criminalized, criminal sanctions should be seen as a necessary or as a necessary evil, as they are in some cases quite justified, no matter the general opinion. With this in mind, an umbrella criminalization might not be the best course of action, as the costs of subjecting every infringer to criminal sanctions might be too much and at the same time, in some cases proper deterrence might be achieved with lesser sanctions. In which cases should criminal sanctions be employed? Due to the high costs of criminal sanctions overall, they should generally focus on situations where the produced benefits are highest while the costs are lowest. Criminal liability should be focused on individual or poorly capitalized infringers who are difficult to detect and identify and at the same time infringe on large quantities of copyrighted materials. This would in addition include large-scale counterfeiting operations which offer bootlegged music, movies, and software.[82] Thus, the most obvious choice for criminal sanctions are those who are actual criminals, who are

[80] Moohr, *supra nota* 76, p 805.
[81] Buccafusco, *supra nota* 66, p 313.
[82] Ibid, p 315 and 316.

indeed doing it for profit and as such infringe on an extremely large amounts of copyrighted material and as such cause the most amount of harm to the copyright owners.

After all of this, it does seem prudent to conclude that criminal sanctions themselves do serve a purpose and as such reverting to only civil sanctions would not in any way provide better deterrence. Having said this, however, an umbrella criminalization would not seem to be a better option either. Some countries have opted to use criminal sanctions in cases where the main aim is to gain profit, which would seem to be the best course of action, as it would not subject the average consumer to criminal sanctions for an infringement which was, for example, done for personal gain. At the same time, this approach would provide enough deterrence for the career criminal who would face criminal sanctions. This approach would then sue civil sanctions against those who would infringe copyrights for personal gain. To achieve proper deterrence, however, the fine would need to be sufficiently high as to actually deter the illegal behavior but at the same time be low enough to not provide a reason for further infringement due to the infringer not being able to pay the fine anyway.

4 Case law

An earlier chapter of the thesis illustrated and described incidents where the DRM system which has been used in a product has in actuality, or potentially might, cause problems for the consumer. The real incidents mentioned in the chapter either were not serious enough to warrant any judicial proceedings, or the issues were amended before judicial proceedings were necessary. This chapter on the other hand focuses on situations where judicial action was deemed necessary. Three different class-action complaints are referenced and analyzed, in which the main causes for concern are related to the inclusion of DRM in the product. The goal for this chapter is to simply illustrate different ways in which a DRM solution may be harmful or problematic to the consumer. Because of this approach, the conclusion of the case is not of any real importance, however it should still be mentioned that in at least one of the cases the DRM solution was found, at least in internal testing, to not pose any problems for gamers.[83]

While the issues, as well as the issues mentioned in the subchapter 1.4., are mainly technical in nature, they are still relevant from the consumer's perspective, as the following chapters detailing each of the class-action complaints should make clear. The cases are from two different industries, one of them being from the music industry and relating to DRM used on music CDs, while two of the cases are from the video game industry. The first of these cases focuses on a specific video game and its DRM, called SecuROM while the second case is focused around a specific DRM solution called StarForce, which has been utilized by Ubisoft Inc in numerous video games. It should, furthermore, be noted that the issues mentioned in these cases are considered to be a problem only to the legitimate buyer. It is said fairly often that DRM only inconveniences the buying user, whereas the pirate, or someone who has obtained the product illegally, is not usually inconvenienced at all, mainly due to the fact that DRM has been removed from the product.

4.1 Spence v. Ubisoft, Inc

[83] Nate Anderson, It's official: Ubisoft dumps StarForce, http://arstechnica.com/uncategorized/2006/04/6603-2/ (accessed 8.4.2016).

The class action complaint against Ubisoft, Inc. revolves around the DRM system StarForce. The claim raises three different problems regarding the DRM: Firstly, titles containing, and subsequently installing the DRM, do not always indicate the inclusion of the DRM[84], secondly the installation of the DRM can compromise the security of the Windows operating system[85] and finally no notice is given to the user that in order to prevent the security compromises, the user would need to remove the DRM and furthermore, in some cases the removal of the title does not remove the DRM software[86]. To back up the first problem of not indicating the inclusion of the DRM, the complaint goes on to give two distinct examples. The first of these examples being, that the End User License Agreement, which the user had to accept before installation did not, in most of the cases indicate that a DRM solution was present[87]. The second example to illust

rate this is a reference to product packaging, which did indicate that the product contained copy protection technology, but full disclosure of the DRM's inclusion was not present anywhere on the packaging[88].

The complaint provides an explanation as to how the StarForce DRM may compromise the security of the operating system. It is stated in the complaint that the StarForce DRM can allow a Trojan or a virus installed on the computer to control it through the DRM, effectively making security measures in newer versions of Windows useless.[89] This is clarified later on in the complaint by explaining that the DRM grants user-level programs access to system level functions which should have been prohibited by a security measure implemented into the operating system[90]. The last matter of the complaint, which concerns the removal of the DRM is explained at length. It is stated that the usual path of uninstalling a product, using the Add/Remove Programs utility in Windows operating system did not always remove the DRM along with the title. It is, however stated that StarForce had provided a separate application which can be used to remove the DRM.[91] The End User License Agreement, which the titles come with, failed to indicate that the removal of the title did not remove the DRM or that a separate application would be needed to remove the DRM[92].

---

[84] California Northern District Court, 3:06-cv-02169, Spence v. Ubisoft, Inc., section 2.
[85] Ibid, section 3.
[86] Ibid, section 4.
[87] Ibid, section 20.
[88] Ibid, section 21.
[89] Ibid, section 3.
[90] Ibid, section 18.
[91] Ibid, section 19.
[92] Ibid, section 20.

The points mentioned in the case may seem minor, however when considering the expectations of the regular consumer, the issues should be fairly clear. The fact that little to no mention is made to the inclusion of the DRM as well as the fact that uninstalling it is not possible by regular means but instead requires a specific application is not something the user can reasonably expect. Similar concerns and issues will be mentioned in the following class action complaint.

4.2 Melissa Thomas et al v. Electronic Arts Inc

The class action complaint against Electronic Arts Inc concerns the video game Spore, and more specifically, the DRM included in the video game, SecuROM. The complaint is based on some of the same problems already explored in the previous case. When installing the product, user is not informed of the automatic and secret installation of the SecuROM DRM program, although the user is made aware that the product does use access control and copy protection technology. Furthermore, it was found that once installed, the DRM program itself will become permanent part of the computer and is uninstallable.[93] The SecuROM DRM, as was the case with previously mentioned StarForce, may weaken the security of the operating system due to how it installs itself[94].

The complaint goes on to explain that Electronic Arts had provided answers to questions about the DRM included in the Spore video game[95], but however had failed to mention that the DRM was a separately installed program. The DRM was referred to as online authentication, which, the complaint claimed, could be interpreted to mean that the DRM protection itself was entirely online-based and no programs would be installed on the user's computer.[96] The matters of uninstallability as well as the security concern are both linked to the same aspect of the DRM: where it is installed. As was the case with the StarForce DRM discussed above, the SecuROM DRM installs itself into the system level, Kernel, which allows it to access all parts of the computer.[97] The fact, that the DRM is installed into the Kernel allows the DRM to effectively control other programs and processes as well as hardware such as DVD-drives of the computer[98]. The complaint goes on to state that once the SecuROM DRM is installed, it

---

[93] California Northern District Court, 5:08-cv-04421-PVT, Melissa Thomas et al v. Electronic Arts Inc. section 2.
[94] Ibid, section 3.
[95] Ibid, section 16.
[96] Ibid, section 17.
[97] Ibid, section 11.
[98] Ibid, section 13.

becomes a permanent part of the computer, and uninstalling it would require completely wiping the hard drive or replacing it entirely[99].

Finally, a problem which is more of a design decision on the DRM part, is that in the complaint it its mentioned that the SecuROM DRM only allows for three authentications in total after which new authorizations would be needed to ask from the Electronic Arts Customer Support, which would give authorizations on a case-by-case basis.[100] This type of issue would mean that should a person need more than three authorizations, for example due to a device theft or computer component upgrades, they would need to contact the Customer Support each time. In these cases, the product could become completely unusable should the user for some reason be unable to get another authorization or if there is no way to unauthorized a computer.

When this complaint is compared to the earlier one, the same themes can be spotted on both of them. In both cases, the user is not made completely aware of the inclusion of DRM and the uninstalling of the DRM may prove to be more difficult than usual or even impossible as is the case here. Both of these cases illustrate that a security concern can exist when dealing with DRM.

4.3 Robert Hull et al v. Sony BMG Music Entertainment Corp et al

The final class action complaint is against Sony BMG Music Entertainment. The complaint is focused around two different DRM solutions, which were used in music CD's. These DRM, which have been used in the CD's are MediaMax and Extended Copy Protection, which is known as XCP. The complaint claims that these DRM solutions among others monitor the listening of the CDs and install undisclosed and hidden files into user's computers which can expose them to malicious attacks without any notice to or consent from the user.[101]

First of these DRM, MediaMax, according to the complaint is installed without any notification to the user and without the consent of the user. What is more, it is told that MediaMax installs eighteen files before the displaying of the End User License Agreement, and

---

[99] Ibid, section 2.
[100] Ibid, section 16.
[101] Superior Court of the State of California, BC343385, Robert Hull et al v. Sony BMG Music Entertainment Corp et al. section 1.

even if the user declines the agreement, the files remain.[102] The complaint states that MediaMax DRM can be uninstalled with an internet-based uninstaller provided by the DRM solution's maker.[103] The uninstaller itself, however suffers from a design flaw, which installs a software component which in turn can allow for malicious code to be run on the system, thus making the uninstaller itself an even greater security risk.[104]

The second DRM to be considered in the class action complaint against Sony BMG Music Entertainment is the Extended Copy Protection or XCP. The XCP does inform the user that it is installing a player software, however the software is installed as a rootkit[105], which is defined as invisible to the operating system and security software and is used to hide among other things files and processes[106].The rootkit, which the XCP DRM installs is reported to degrade the performance of the computer[107]. To further explain the severity of rootkits in general, the complaint explains that rootkits by nature are extremely difficult to remove from a computer, which often leaves reformatting the entire hard drive the only option of getting rid of a rootkit. This then would require the user to re-install the operating system and all the programs and drivers which could take hours and might very well be beyond the technical capabilities of some users.[108]

As can be seen here, the issues in these three cases have been fairly similar. The user has either not been aware of the inclusion of DRM at all, or the installation is somehow different to what the user could expect. Furthermore, the uninstalling of the DRM is either extremely difficult or impossible. While these issues are mostly technical in nature, they should nevertheless indicate that DRM can have serious shortcomings which in turn can have serious effects on the user-experience and even result in a security risk.

---

[102] Ibid, section 20.
[103] Ibid, section 36
[104] Ibid. section 37, 39
[105] Ibid, section 50.
[106] Ibid, section 51.
[107] Ibid, section 53.
[108] Ibid, section 66.

5 DRM Circumvention

Now that the issues concerning DRM implementations have been established in full, it is time to turn our attention to a possible solution or solutions. There should be no denying that issues with certain DRM implementations exist. In the introduction it was mentioned that the other research question of this thesis is, whether DRM circumvention should be legal in some cases and that is indeed one of the solutions to these problems the author wishes to propose. From the perspective of the consumer, DRM is a nuisance, and the most obvious and easiest solution would be to provide everything DRM-free, effectively completely removing DRM form the equation. However, while DRM-free products are in the market and some buy them more than others, it is still only a part of all the products being sold. Copyright itself is something which should be taken into account when thinking about DRM and exactly because of copyright and everything it entails; DRM is here to stay in some form at least. This does not mean that there can be no change to it, which is why the author believes that DRM circumvention should be legalized in some cases, and most importantly it should be legal to only those who have legally purchased a product with DRM. Those who pirate the products should still be held accountable.

5.1 Prohibition of circumvention

Earlier in this thesis, it was established that protection of technological protection measures has been split into two different directives in the European Union, while in the United States the Digital Millennium Copyright Act is relevant. Before discussing whether something should be allowed or not, it would be a good idea to discuss what is actually prohibited. In an earlier chapter, it has been already established that DRM circumvention in regards to computer programs is illegal due to license agreements which accompany video games. When it comes to the InfoSoc directive, however, different Member States have implemented the circumvention prohibition differently, while some have even allowed circumvention in very strict cases. In Denmark for example, intentional or negligent circumvention of technological protection measure results in sanctions under general tort principles[109], while in France, Germany and the UK it is not certain whether the act of circumvention is enough or whether a subsequent

[109] Westkamp, G. *supra nota* 19, p. 54

infringement of copyright is required.[110] The common starting point, however, seems to be that circumvention is characterized as a general matter of copyright law and because of this circumvention itself becomes an offence only when an infringing act results. This then excludes circumvention when it is carried out in order to view, read or listen to a work which allows the circumvention in cases of regional encodings on DVD's.[111]

Whether this actually means that circumvention could already allowed in cases where the DRM software makes it impossible or difficult to view, read or listen to the work or whether it only applies to circumventing of DVD region coding is debatable. Relating to this, it would seem that in Norway and Denmark this exception does imply that it would be allowed to circumvent measures to rip tracks from a CD into MP3 format or even remove measures which would then allow a work to be played on a different MP3 player.[112] Regarding the possibility to circumvent DVD region encoding, the preparatory documents relating to the Finnish Copyright Act and its implementation of the InfoSoc directive state that the protection of article 6 (1) of the directive only applies to those technical protection measures which can be used to prevent or restrict access to protected works and because of this, DVD region encoding and its circumvention is not an act which would be prohibited. The circumvention nonetheless cannot result into making another copy of the work.[113] It would then seem, at least if the above is indicative of the common sentiment in the European Union, that allowing circumvention of only DVD's and their region encoding is indeed the only exception and that extending the exception to other cases is not all that widespread. What this would indicate is that DRM itself, as its main goal is actually to restrict and/or prevent access to a work is protected by the article 6 (1) and circumventing it would be prohibited, except when it explicitly is not, as was mentioned earlier in the cases of Norway and Denmark.

Geo-blocking was described as a relatively new form of DRM in an earlier chapter, its newest iteration being utilized by streaming services such as Netflix. The main issue with geo-blocking and considering its circumvention is that the internet is commonly seen as a borderless space, without any central authority. Corporations and governments are trying to partition it, by geo-blocking, into areas which mirror territorial borders. Circumvention of geo-blocking may very well increase, as more and more content is blocked behind geographical walls.[114]

---

[110] Ibid. p 55.
[111] Ibid p 56-57
[112] Ibid. p 57
[113] HE 28/2004 vp, Hallituksen esitys Eduskunnalle laeiksi tekijänoikeuslain ja rikoslain 49 luvun muuttamisesta, p 124.
[114] Kra-Oz, *supra nota* 38, p 20.

The very real problem with geo-blocking in this age is that the internet does not truly know no borders and geo-blocking is an artificial way of enforcing these borders on users. Some might feel the need to circumvent these borders, which is in actuality extremely easy. Circumvention can simply be done by rerouting one's IP address through a server in another country, either by using a proxy or a VPN service, and thus seeming to originate from the country where the server resides. Whether this is actually legal, is a completely another matter. While there does not currently seem to be case law outlawing geo-blocking circumvention, multiple legal dimensions can still be taken into account when discussing it.[115] As was the case with DRM circumvention and computer programs, circumvention of geo-blocking can constitute a breach of contract, as the service utilizing geo-blocking can easily prohibit circumvention in the terms of service. Netflix for example states in its terms of service that the service is meant to be used primarily in the country where the account has been established, and that the service uses technologies to establish the user's geographic location.[116] Another aspect which needs to be taken into account when discussing circumvention of geo-blocking is legislation. Both the WIPO Copyright Treaty and the Digital Millennium Copyright Act provide protection to technological measures and prohibit its circumvention. In the United States, however, there has not been any real answer as to whether copyright infringement must follow circumvention in order for it to be illegal or not. Another issue entirely is whether geo-blocking is used to enforce copyright or not.[117]

Computer programs in the European Union are protected by Directive 2009/24/EC on the legal protection of computer programs. It was earlier established that some countries consider video games to be computer programs while some do not. Article 4 (1) (b) of the directive restricts the translation, adaptation, arrangement and any other alteration of a computer program.[118] Article 5 of the directive provides exceptions to these restricted acts. It is stated in Article 5 (1) the acts in article 4 (1) would be allowed in the absence of specific contractual provisions if they are necessary for the use of the program by the lawful acquirer in accordance with the intended purpose, which would include error correction.[119] It would seem then, that circumvention of DRM would be allowed in cases where it would be needed for the product to attain its intended purpose. However, video games are accompanied by an End User Li-

[115] Ibid p 21.
[116] Ibid p. 22
[117] Ibid p. 23
[118] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L111/16, article 4 (1) (b)
[119] Ibid, article 5 (1).

cense Agreement, which may prohibit modification and/or alteration of the content. The popular video game store and service Steam by Valve has a subscriber agreement, in which the user agrees that they "may not, in whole or in part, (…) reverse engineer, derive source code from, modify, disassemble, decompile, create derivative works based on, or remove any proprietary notices or labels from the Content and Services or any software accessed via Steam without the prior consent, in writing, of Valve."[120] Another example of a license agreement which effectively prohibits DRM circumvention is the Software License Agreement for the video game Wolfenstein, in which it is stated that it is prohibited to "remove, alter, modify, disable, or reduce any of the anti-piracy measures contained in the Software, including, without limitation, measures relating to multiplayer play."[121] Steam being a service which sells many video games and software, these restrictions apply to everything accessed via Steam. The second example shows, that these types of license agreements are not only used by large gaming websites and webstores, but by individual videogames themselves. If these types of agreements are considered to be specific contractual provisions in the meaning of the legal protection of computer programs directive article 5 (1), then they would effectively make the exception useless as regards to DRM circumvention and if this was the case, it would seem that DRM circumvention would be considered illegal in the European Union at least when video games are concerned.

5.2 Exceptions to prohibition of DRM circumvention

Last chapter established that circumvention is indeed prohibited, whether it is against legislation or due to contractual provisions. This chapter focuses on the possibility that DRM circumvention could be illegal. It should be said, that due to copyright's existence, the circumvention should only be limited to cases where the legal purchaser has a problem with the product due to DRM inclusion. While some issues regarding DRM have been established, what could legally justify the legalization of circumvention? There has been a case regarding DRM interoperability in Norway against Apple and its iTunes terms of service. The complaint, which was filed with the Consumer Ombudsman by the Norwegian Consumer Council was based on an Act

[120] Valve S.a.r.l., Steam Subscriber Agreement, http://store.steampowered.com/subscriber_agreement/ (accessed 14.4.2016)
[121] Wolfenstein Limited Use Software License Agreement Section 3 (m)

which allowed the Ombudsman to intervene and prohibit the use of unfair terms and conditions in consumer contracts.[122] It would them seem, that consumer protection legislation could be used at least to some extent to justify the legalization of circumvention. In the aforementioned case the Ombudsman stated that the agreement which iTunes used was unfair due to forbidding the removal of DRM and locking consumers into Apple's ecosystem[123]. This further proves that consumer protection laws could actually have some sway against DRM. It would seem, at least according to that one case, that in Norway terms of agreements should not be unfair, which is what forbidding DRM removal seemed to be. The problem, when it comes to digital products is whether they are actually goods. In the United Kingdom, if the software is considered bespoke, it is regarded as a supply of professional services, however when other digital products are sold off-the-peg, the situation is not so clear. Some believe that as digital products are intangible they fall outside the definition of goods, while others believe that the definition of goods is elastic enough to fit digital products beside tangible goods which would give digital products the same protection.[124] Additionally, the European Directive on Consumer sales and Associated Guarantees defines goods as tangible movable property, which however does not answer the question of what tangible is and if it requires that goods have a physical presence and can be touched.[125] The Norwegian case referenced above would, however indicate that at least to some effect digital goods could indeed be considered goods and consumer protection acts could be applied.

The Finnish Consumer Protection Act defines consumer goods as goods which natural persons acquire for their private households as opposed to a use for business or trade[126]. Chapter 5 of the Consumer Protection Act is focused on sale of consumer goods. Section 12 of Chapter 5 is titled General provision on defects. Article 1 of section 12 states that goods should correspond to that what has been agreed.[127] This could possibly apply to situations where the consumer has not been made aware of DRM implementation in the product. Article 2 subsection 1 states further, that if nothing else has been agreed, the goods should be fit for the purpose which they are ordinarily used.[128] With this in mind, it could be argued that products where DRM somehow hinders or even makes impossible the usage of the product, would be in fact

---

[122] Valimäki, M. *et al.* DRM Interoperability and Intellectual Property Policy in Europe, European Intellectual Property Review, 28(11) 2006, p 567
[123] Ibid.
[124] Bradgate, R. Consumer Rights in Digital Products, UK Department for Business, Innovation and Skills, Institute for Commercial Law Studies, University of Sheffield, September 2010, p 61.
[125] Ibid p. 66.
[126] Kuluttajansuojalaki 38/1978, Ministry of Justice, chapter 1, section 3
[127] Ibid, chapter 5, section 12, article 1
[128] Ibid. chaper 5, section 12, article 2, subsection 1

defective. In the cases of defective products consumers do have other courses of action, such as returning the product or getting the product repaired, however in these cases where DRM is at fault and if the developer of publisher does not for some reason or the other wish or is unable to assist, circumvention could be a way to still retain the product while at the same time being able to use it properly as it was meant to be used. Chapter 3 of the Consumer Protection Act regulates contract terms, like those which came to question during the iTunes case discussed above. Section 1, subsection 1 states that no contract terms should be used, which are deemed to be unfair taking into consideration the point of view of consumers.[129]

While these are an example of only one country's Consumer Protection legislation, they should nonetheless make it clear that in some ways, that same legislation could be applied to cases where DRM is causing issues. As was mentioned, other ways of fixing the issue of a defect in the product are available to the consumer, however, allowing for circumvention could potentially keep the sale of the product and keep the consumer happy when the only real possibility, when no repair in these cases is possible, would be a refund of the product. Another aspect, which would require contemplating is the matters of unfair contract terms. In the Norwegian iTunes complaint, it was noted that contract terms forbidding the removal of DRM were considered unfair. From this point of view, then it could be said that agreements which prohibit circumvention are themselves against consumer protection acts, which then would make circumvention legal.

Finally, something to consider is reverse-engineering. What is allowed, and what is relevant considering the topic of DRM, is making modifications. Modifications for example could be bug fixing or enhancing the program which allows it to work better. It has been ruled at one time that the modifications are permitted, however, only if they are necessary for the software to be executed, while on another occasion it was ruled that modifications were allowed to make the software more usable for the purposes it was acquired.[130] While reverse-engineering itself could be considered to be legal, it is effectively prohibited in the contract terms employed by the software sector.[131] It would then seem that circumvention of DRM could theoretically be allowed if it was considered to be modification under reverse-engineering. The fact that reverse-engineering is prohibited under contract terms is an issue, and thus allowing it would

[129] Ibid. chapter 3, section 1, subsection 1
[130] Samuelson, P. Reverse-Engineering Someone Else's Software: Is it legal?, IEEE Software, January 1990, p 94.
[131] Bechtold, supra *nota* 25, p 365.

require changing the contract terms or perhaps making such terms null and void at the outset. Whatever the case, and whichever the method of allowing DRM circumvention, the required changes would by necessity need to pass both the legislator's desk as well as get the approval of all of the industries who come to contact with DRM. Whether this is actually doable, and if the industries actually would approve of allowing DRM circumvention is an entirely another matter.

Another matter which should be discussed is that some DRM simply cannot be circumvented while still retaining the ability to use the actual product. Some video games, for example require an internet connection to actually work, which might be due to online components in the game or something similar. These online-requirements have become more and more prevalent recently, while at the same time the issues have become more widespread. As a secondary way of fixing these problems, if circumvention is not possible or feasible, some sort of standardization or at the very least some minimum requirements which DRM should fulfil should be a possibility. The EU Directives and other legislation governing technical protection measures do not in any way say anything about any type of minimum requirements which the DRM should fulfil. These are then simply anti-circumvention legislation and as such when issues arise, they are dealt with on a case-by-case basis relying on other legislation, when they could quite easily be dealt with before the issues even surface. This could easily be done by standardizing TPM's and RMI's and with that, DRM to such a degree that those employing DRM in their product would need to make sure that the software or hardware limiting access does not pose any type of threat or issues to the users in terms of them actually enjoying the product. Should these problems nonetheless arise, the user could then go about circumventing the DRM or the developer, supplier or creator of the content could supply them with a circumvention device on a case-by-case basis provided of course that the user is a legitimate buyer.

5.3 EU Digital Single Market

While the European Union has had a single market for quite a while now, it has not been true for digital content. Geo-blocking has blocked content to certain geographical areas even within the European Union giving little regard to the single market. Thus, the goal and ideology of a true single market, even within the internet has not in truth happened. To make this goal a reality, however, the European Union has set out to extend the single market into the digital world with the European Union Digital Single Market strategy. Granted, the digital single market does not necessarily touch all the issues or even all the different types of DRM which have been used and will be used. Most likely to only DRM solution to actually feel any type of change due to the digital single market is geo-blocking, as the goal is to abolish all

the digital borders within the European Union and thus effectively abolish geo-blocking within the EU. The impact itself may seem minuscule when compared to everything which has been discussed in this thesis and true enough, it is a small change but at the same time it is a small, but important, step in the right direction. If these changes are executed correctly and received well, both by consumers themselves and by corporations utilizing DRM, the next step could quite possibly be a much larger one.

The European Commission's Digital Single Market strategy is based on three pillars and 16 key actions. Out of these three pillars, the first one, better access for consumers and businesses to digital goods and services across Europe, is the most interesting one considering DRM and specifically geo-blocking. Under the first pillar, eight measures are proposed by the Commission out of which the first one deals with rules to make cross-border e-commerce easier while the fourth one would dictate and end to unjustified geo-blocking, which is seen as a discriminatory practice.[132] While ending geo-blocking is of course extremely important, the first measure is of some importance as well, mostly because these measures to some extent complement each other. Ending geo-blocking should by design bring the same content, and the same amount of said content, to the fingertips of everyone while before it was only accessible to a fraction of the populace of the European Union.

While the previously mentioned measures and pillars were a part of the European Commission's strategy, the European Parliament additionally has something to say in the matter. The Parliament supports a revision of the InfoSoc Directive, which is another step towards a digital single market. The resolution does specifically mention geo-blocking in the vein of asking the Commission to deal with cross-border accessibility which is tied to portability of services and access blocking which is tied to a user's geographical location[133]. While the recognition of the issue of geo-blocking is excellent news, the Resolution seemed to promote territoriality to a degree, which is in direct conflict with removing geo-blocking. It is mentioned in the Resolution that copyright itself, and all the related rights imply territoriality, however currently territoriality is a requirement due to how different rights are cleared in the European Union, which is on a country-by-country basis. Another issue with the proclamation that copyright inherently means territoriality is that the establishment of a unified copyright law for the entire Union is not in any way prohibited by the international intellectual

---

[132] Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen, EU Focus, 332, 2015, p 1, 2.
[133] Geiger, C., et al, The Resolution of the European Parliament of July 9, 2015: paving the way (finally) for a copyright reform in the European Union?, European Intellectual Property Review, 37(11), 2015, p 686.

property framework. Which then would clearly imply that territoriality is not in any way linked to copyright.[134]

The Commission's strategy seems to be fairly favorable towards abolishing digital borders and with them geo-blocking within the Union. The Parliament on the other hand, while still thinking the issue is a problem and even going so far as to asking for the Commission to deal with it but at the same time they are, in the same Resolution, promoting territoriality to a degree which seems fairly controversial. The issue with geo-blocking, and at the same time the road towards a digital single market, is that there is no middle ground: either the content is geo-blocked or it is not, and because of this the fact that the Parliament at the same time wants to get rid of geo-blocking and wants to promote territoriality does not make sense. Furthermore, if the digital single market is to reach its true potential and actually become a true single market, the territory restrictions would need to be brought down. Thankfully the Commission's strategy is at least favorable and would indicate that geo-blocking at least would be a thing of the past in the European Union. It would then seem that the European Union Digital Single Market could actually help the situation with DRM, or at the very least it could be the first necessary push towards a slightly better application of DRM.

[134] Ibid p 685.

6 Conclusion

During the last 15-or so years, the internet has become an ever-increasing part of our lives. The internet has, among other things, allowed us to transfer large amounts of data from one corner of the world to the other corner in a matter of minutes or even seconds. This has, ultimately, led to a certain type of digital revolution with different types of products, ranging from movies and music to video games and even e-books being sold digitally. While internet has allowed for the swift transfer of data, it was the digital files themselves which are actually the root cause of the problem. Data is extremely easy to copy and as a consequence, making exact, carbon copies of products is extremely easy and fast. When this easy reproduction of data, and essentially products, is combined with high-speed internet, the resulting combination means that a product may be copied and spread around the world with ease. This is a combination which is very good for content creators, as they can have one single copy of a certain product and multiple people can then buy the product, thus eliminating the need to press actual physical books, DVD's or music CD's. The aforementioned combination unfortunately in addition works for illicit means, as the digital product is easily reproduced and transferred to users around the world who can pirate the product without actually paying for it. This issue of piracy, and making of illegal copies is against the copyright of the author of the product and is then against intellectual property law.

Piracy has resulted in certain technical protection measures being added to digital products, which are usually referred to as Digital Rights Management, or DRM for short. The main purpose for DRM is to restrict or deny access to a product in such a way that only a person who has legitimately purchased the product has access to it. This has been addressed and achieved in various ways over the years. DRM has been used on for example movie DVD's, music CD's and eBooks. DVD's for example relied on regional encoding, an early form of geo-blocking, which limited a DVD to a certain region and that DVD could only be played on a DVD-player which was bought in the same region. Video games on the other hand have often relied on some type of key-based authentication method. The authentication relied on a key of some sort, usually an alphanumeric string which would be input during the installation procedure. Originally this key would then be compared to a set of rules within the installation disc itself, which proved to be easy to circumvent and illegitimate keys were easy to generate and duplicate keys could be used. To remedy this, offline authentication was replaced by online-authentication in which the key was compared to a list of keys on an online server, which made it impossible to use duplicate keys and made it more difficult to generate illegitimate keys. This eventually led to the requirement of a constant internet connection for authentication for not only video games but some streaming services as well.

While the goal and purpose, due to reasons explained above, of DRM is justified and legitimate, the implementation has not always been flawless. DRM has resulted in issues for users on numerous occasions, while some even resulted in class-action lawsuits in the United States. Geo-blocking for instance restricts bought content to a certain geographical area, thus by design, should a person travel to another area, the bought content may not anymore be available to the consumer. Similarly, some DRM solutions may restrict content to a specific device, while recently more and more services, such as streaming services, have begun to restrict content to a user-account. DRM solutions which require a constant internet connection have caused much trouble for consumers as the product and the servers attached to it have not always worked perfectly and due to connectivity issues the product has been unusable for those who have legitimately bought the product. Finally, some DRM implementations have suffered from interoperability issues, where for some reason or the other the product no longer works, be it due to an incompatibility due to a newer operating system on a computer or some other such issue.

These incompatibility, and other, issues can be solved by the most part, by circumventing the DRM solution entirely. Thus, this thesis sought to answer two different research questions, firstly whether DRM circumvention could and should be legal and secondly whether the blanket criminal sanctions for circumvention in force in some countries are actually effective or whether there is another way. The answer to the first question was achieved by first establishing that circumvention was in the current legislation actually illegal. Legislation, which concerns DRM, and which are often referred to in this thesis are in the EU the InfoSoc directive and the directive on legal protection of computer programs and in the United States the Digital Millennium Copyright Act or the DMCA. All of these pieces of legislation contain provisions which are said to be anti-circumvention in that they prohibit circumvention of technological protection measures. While some exceptions exist, they were found to be ineffective, mostly due to contractual provisions which usually accompanied the digital products. It was thus found that circumvention is illegal.

Legal reasons for allowing circumvention were mainly searched from consumer protection legislation, while taking a look at an ombudsman complaint from Norway, in which it was stated that prohibiting DRM removal in a case where the DRM restricted the playing of music to only Apple products was found to be an unfair contract term. As it was established that consumer protection legislation could be applied, the Finnish Consumer Protection Act was then searched for relevant articles which could be applied to various problems with DRM. It was found that provisions concerning defects in a product could possibly be applied to issues caused by DRM and furthermore provisions concerning unfair contract terms could be applied to cases where contracts prohibited DRM circumvention. Circumvention was posed to be a way to keep both the consumer and the content provider happy, as circumvention would allow for the consumer to keep the product and still use it, where otherwise a return of the

product could have been the only option previously. As an option to circumvention, due to cases where it would not have been possible without actually compromising or making the product unusable an alternative solution was suggested: standardization. Currently no minimum standards for DRM exist, and thus no real responsibility lies on the company when they choose which DRM to utilize. Standardization, or setting some sort of minimum standards at least, would ensure that the DRM utilized would not be too intrusive and would work relatively well without too many issues. The hypothesis for this question fairly well reflected what was found eventually. Circumvention could in theory be legal, however whether that actually comes to pass, and more importantly whether copyright holders agree is an entirely different matter. While some legislation was found which potentially could apply to DRM circumvention's legalization, the topic nonetheless is still extremely hypothetical at this point.

The second research question this thesis sought to answer was what type of sanctions there are for DRM circumvention. Additionally, the sanctions and their effectiveness were analyzed in a cost-benefit manner. Legislation, which was utilized was the DMCA regarding sanctions in the United States, while in the European Union InfoSoc directive was mostly used. During the research it was found that the implementation of the InfoSoc directive varied wildly between the Member States in the EU, thus different variants of sanctions were imposed on infringers. Some Member States straight up imposed criminal sanctions, some imposed criminal sanctions only on those circumventing for profit while a few chose to not impose criminal sanctions at all, favoring civil sanctions instead. The DMCA in the United States is based on both of the WIPO Treaties, the Copyright Treaty as well as the Performances and Phonograms Treaty, thus the DMCA has sanctions concerning circumvention. Criminal sanctions would be imposed according to the DMCA if the offense was done willfully and for financial gain, both business or private. Next, the effectiveness and usefulness of criminal sanctions was under scrutiny. Sanctions on general piracy were found to be fairly high on some occasions, with the fine going up as the amount of pirated content itself increased. When criminal sanctions are then regarded, the amount of fines awarded tends to go even higher. It was found, that those facing criminal sanctions for whatever reason might be unable to pay the fines in any reasonable manner. This coupled with the fact that the person facing these charges could be a person with very little disposable income, and the fact that if a person is facing charges of thousands or possibly hundreds of thousands of euro's and is unable to pay them, nothing is in truth stopping them from infringing on copyrights for a few thousand euro's more.

Another aspect which was considered was that criminal sanctions, while effective in some cases, are fairly costly. If the ultimate punishment, incarceration is used, the cost of the incarceration will be borne by the society. Finally, it was found that criminal sanctions may in fact be over-deterring in more ways than one, as they could very well deter valuable behavior as well. Those fearing high sanctions could very well refrain from socially valuable circumvention and copying acts, such as where the act would actually be allowed. It was, however,

found that criminal sanctions do have a use, as in some cases incarceration may be the only possible sanction which has a high enough deterrence. This was found to be true exceptionally well for those who infringe on copyrights professionally, i.e. who do these acts for profit. For these people, the only real deterrence is actually the loss of freedom, instead of something monetary. Criminal sanctions do not necessarily have to mean incarceration, however, as alternative sanctions were discovered, such as temporary prohibition to use technological devices. This would effectively stop the infringer, but would not burden the society with high incarceration costs. Overall, criminal sanctions for common people, who do not infringe on copyrights for profit, were found to be overkill, as the possibility of over-deterrence is real, and at the same time civil sanctions could prove to be the right balance as the fines would not necessarily be too high to cause over-deterrence but at the same time the person infringing would still have something to lose when infringing on copyright.

Finally, the thesis looked into the forthcoming EU Digital Single Market. It was found that both the Commission and the Parliament had submitted documents relating to the digital single market, with varying degrees of success. The overall idea of digital single market was found to only really affect geo-blocking, while other forms of DRM were left out. However, the Commission's strategy was found to be extremely favorable towards abolishing geo-blocking entirely within the European Union while at the same time making cross-border e-commerce easier. The European Parliament's Resolution on the other hand, while still being fairly positive about abolishing geo-blocking, at the same time seemed favorable towards territoriality which is at the complete opposite direction from abolishing geo-blocking. Overall, however, the effects of the digital single market are still unknown and whether any impact will be had on DRM remains to be seen.

7 Digitalization and DRM in a corporate setting

The above thesis was written roughly two years ago, from the writing of this chapter, for a bachelor's degree in law. This chapter was written to fulfil the requirements of accreditation towards a bachelor's thesis in business management. Thus, this chapter will focus less on the legal side of DRM, and more on the practical application of DRM from a business perspective, and on digitalization and its effects on business in general. This extension to the thesis wishes to explore how and why DRM should be utilized from a business perspective, and secondly how has digitalization started to show in the business landscape and how does DRM fit into this new digital world.

It should be noted, that from a legal point of view not much has changed since the writing of the original thesis. The same directives and pieces of legislation are still in force in the EU, and as such the judicial discussion is still very much valid. This is not to say that the last two years have been for nothing, as the Digital Single Market initiative of the European Union is still very much moving forward and signs of that are very much visible in the abolishing of roaming charges within the Union and indeed, the coming into force of the General Data Protection Regulation, which both aim to make the digital lives of the EU citizens that much better. It should be noted, however, that while both the GDPR and the roaming charge abolition were positive for the consumers, this was most definitely not the case for businesses, as both changes create significant extra costs for businesses. Digitalization, of course, creates additional expenses, but it does also create more opportunities.

As has been already discussed at length above, DRM is a form of protection to be used against unlawful use of digital products. This, inherently, makes DRM a tool for those who wish to sell digital products, such as films and music. Companies all around the world have embraced digitalization wholeheartedly, bringing digital delivery solutions to many industries, such as film distribution, music distribution and now even modern cars get their firmware updated through the internet. Unlawful use of digital products is an issue, and DRM is one answer to the problem, which makes the usage of DRM a business decision: can we gain more from the usage of DRM than we lose by using it? It has been already mentioned, that some digital distributors use the fact that they do not have DRM included in their products to their advantage, while others view the risk of unauthorized use as a more pressing concern and implement DRM in some way or another.

7.1 DRM in a business setting

The thesis has so far mainly focused on DRM from the consumer's point of view, but DRM is not usually used by consumers, but businesses. Thus, the decision of whether to use DRM or not is always a business decision, because the main goal of using DRM is to protect something from unwanted access or use. DRM usage from a business perspective seems at first an obvious choice, however considering what has already been said above, the decision should be properly weighed against both the business' values as well as the cost-benefit of implementation.

The film industry is an interesting example, because it captures both the consumers directly, and other businesses, namely cinemas. From the consumer's point of view DRM can, and often has been, a problem, because it makes the in-home or on-the-bus viewing experience a hassle if access management does not work properly for some reason and thus they cannot view the film they've bought.

Conversely, in a business-to-business setting, DRM implementation of course is used to restrict access, but it does not hinder the consumer or the cinema as much. Implementing DRM into the digital film release allows the distributor to curb early showings of the film by limiting the access to the film only after a certain date, limit the showings of the film to certain days and hours or to a certain date range[135]. This gives the distributor more control over the viewings, and the ability to charge a fee per viewing, which has not been as easy before. This is one example of how the usage of DRM can vary between use cases, and that DRM can indeed be a worthy business decision, as long as it has been implemented properly. This does not mean that all consumer DRM implementations are bad, or that all business-to-business DRM implementations are worth it, but this simply illustrates that there are two sides to the same coin. Something that should also be kept in mind, is that especially when upgrading from analog film cinema to digital solutions, the costs of implementation can, and in most cases will be, high. Thus, even though for the film industry, the switch to digital may have been beneficial, there are always two sides to the coin and in this case, cinemas had to invest in new projectors and equipment to keep up with the evolution.

---

[135] Peinado, M., et al, "Digital rights management for digital cinema", available at: http://www.petitcolas.net/fabien/publications/acmmm03-cinema.pdf, p 4

The original thesis has examples of how the usage of DRM can be harmful, however this chapter attempts to show DRM from a business perspective, and thus give the reader a more balanced view of DRM, in order for them to make an informed decision on whether DRM could suit their business. The above cinema example is a good example of how DRM can be utilized in a business-to-business setting. In a business-to-customer setting, the company would need to consider what has been said in the rest of the thesis more thoroughly, because the consumer aspect brings more responsibilities and risks into the equation. Both of these cases do hinge on the fact that whoever would be using the product utilizing DRM uses the product or invests into the equipment required to use the DRM protected product, as in the cinema case. Thus, while it may seem easier to justify, and implement, a DRM protection in a business-to-business setting, there may be more costs incurred by the user, especially if new equipment is needed.

In a business-to-consumer setting, a company would need to be careful when considering DRM implementation, as the implementation directly affects how the consumer is going to use the product. As has already been mentioned, a mishandled implementation could potentially lead to a inoperable or unusable product, when the consumer has expected for the product to work or be available. If a company nonetheless wishes to use DRM, they should choose the less intrusive one, or one that would be best suited for their product while keeping all the possible use cases in mind. If the product, and its users, are only in one location or country, the DRM could for example limit the use to that certain geographic area. There have been many cases where geographical DRM has been an issue, however, and these risks should also be weighed against the possible, or actualized, gain. Another aspect, a customer-oriented company should keep in mind is with what kind of device the customer could potentially interact with the product, as this can severely limit the possibilities of DRM utilization. A purely web-based product does not need much in terms of DRM, as the need for an internet connection and perhaps an account of some sort should be enough to restrict access to legitimate users only, but if the user can somehow download the product to their own device, a more robust DRM implementation will be required.

For a purely business-to-business company the situation is slightly different, even though the company would need to keep the same aspects in mind, as the user could still face the same issues as a regular consumer. In a B2B scenario, one could even argue that the standards are even higher than in a B2C setting, as the business who uses the product could very well depend on the availability of the product and that it works as advertised. In the cinema example above, the cinema would be practically unable to do business if the licensing system would not work properly, as they would not be able to show any films to their viewers. In such a case, both the business and the consumer would be affected by the implemented DRM. In a purely B2B setting, where the consumer is not directly affected the DRM, the effect may not

be that severe, but it could nonetheless affect the customer company's business in a harming way.

While the negative effects of DRM are substantial, the gains from using DRM can be substantial as well, as long as both the negative and positive effects of implementation are weighed, and the implementation itself is done properly. In a best-case scenario, DRM implementation can allow the company more control over its products, without hindering its usage. Using DRM just for the sake of using it should not be the sole reason for using it, but instead the proper reason for using a DRM solution should be thought through thoroughly, as DRM can only be a viable method if the company recognizes the need to use DRM but also knows what risks they are trying to mitigate with DRM. While DRM has been used in a B2B setting, it is nonetheless a more prominent way to secure products for B2C companies, because consumers are more prone to acquiring digital products through illicit means. Companies on the other hand should not see piracy as an option, as it could tarnish the reputation of the company and prevent it from doing business in the long run. Furthermore, with business editions of software, or digital products, often comes support and other value-added functionalities that could prove to be more helpful to companies rather than the money saved when unlawfully acquiring the same product.

Considering how widely the use of digital products, and their adoption by the general public, has spread in the last 10 years, it can by now be said with some certainty that the digitalization of the world is well on its way. The extent of digitalization is something one can only guess at this point, but the age of physical mediums such as CD or DVD, is if not over, then at least giving way to a more digital tomorrow. With digitalization, companies are facing new hurdles, among them the protection of their digital products. With this in mind, DRM does have a justifiable reason to exist and companies are entitled to protect their products from unlawful usage. What this chapter, and this thesis, has attempted to impart on the reader, is that while a company has a justifiable cause to utilize DRM, they should also take into consideration how DRM can and will affect the user and how the different DRM implementations affect the usage of the products and restricts the access. Thus, a proper risk-benefit analysis should be conducted while also keeping in mind what kind of users does the product target, and whether the implementation should be robust enough to not restrict another company's ability to do business should they buy a product with DRM.

7.2 Digitalization

Digitalization as such is a much larger topic than whether or not a company should or should not use DRM. DRM is the effect, whereas digitalization is the cause. The concept of digitalization in a business setting is and interesting one, because it can mean different things to different business entities. The simplest forms of digitalization could very well simply be to upgrade from a central server which the company owns itself to a server infrastructure service provided by a third party. At the same time, digitalization could mean the research and development of a new digital product related to the industry the company is in. The latter would most likely need DRM, whereas the former would not.

From the point of view of a company, digitalization is an investment. An investment on a new medium, a new way to deliver products, or a new way to approach their customer base. Digitalization means the abolishing of the traditional ways of shipping or delivering a product to the customer, because with digital products there is no physical product that would need to be delivered. The above example of the new digital delivery of movies to cinemas is an excellent example of digitalization at its finest, because in this case digitalization makes both the production and the shipping of film reels to cinemas a non-issue. It is entirely possible that films are still delivered to the cinema in some form, whether on a hard-drive or similar storage device, which would not entirely defeat the need to deliver something physically to the theatre but at the very least hard-drives do not have to be specially made for the movie but can be bought anywhere. At the same time, it could very well be possible for the movie to be delivered entirely through an internet connection if this was found feasible.

If we were to link digitalization to the rest of this thesis, it could very well be said that digitalization is the investment, which the company wishes to make, whereas DRM is a way to protect that investment. This line of thinking is indeed completely understandable, especially if the product, or whatever the investment may be, is a completely new venture for the company. Protecting their new and exciting, but also frightening, foray into the digital world needs robust means of access-control simply because digital products are extremely easy to copy and use without authorization. Who can then blame those who would wish to make sure that their investment has not been in vain, and who would wish to reap the profits from their investment? Here, once again, we come to the question of cost-benefit analysis. A business is nothing without its customers, and unless the company has a monopoly, there are always other companies to which the consumer can turn to, and this is why companies should take their digital investments seriously and also consider how their actions might affect the consumers, and how their product could be best both secured against unwanted access but

also give unhindered access to those who have bought their product and believed in their investment.

8 Reference list

Articles

1. Akester, P., The impact of digital rights management on freedom of expression - the first empirical assessment. *International Review of Intellectual Property and Competition Law*, 41(1), 2010, p 31-58.
2. Akester, P., The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture. *European Intellectual Property Review*, 32 (8), 2010, p 372-381.
3. Bechtold, S., Digital Rights Management in the United States and Europe. *American Journal of Comparative Law*, Spring 2004, p 323-382.
4. Buccafusco, C., *et al*., Innovation and incarceration: An economic analysis of criminal intellectual property law. *Souther California Law Review*, January 2014, p 275-334.
5. Bradgate, R. Consumer Rights in Digital Products, UK Department for Business, Innovation and Skills, Institute for Commercial Law Studies, University of Sheffield, September, 2010.
6. Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen, EU Focus, 2015, 1-3
7. Dubbelde, J. J., A potentially fatal cure: Does digital rights management ensure balanced protection of property rights? *University of Illinois Journal of Law, Technology and Policy*, Fall 2010, 409-432.
8. Favale, M., Fine-tuning European copyright law to strike a balance between the rights of owners and users. *European Law Review*, 33 (5), 2008, p 687-708.
9. Fetscherin, M., *et al*, Comparing the Usage of Digital Rights Management Systems in the Music, Film, and Print Industry, ICEC '03 Proceedings of the 5th international conference on Electronic commerce, 2003
10. Geiger, C., *et al*, The Resolution of the European Parliament of July 9, 2015: paving the way (finally) for a copyright reform in the European Union?, European Intellectual Property Review, 37(11), 2015
11. Hardy, T., Criminal copyright infringement. *William & Mary Bill of Rights Journal*, December 2002.
12. Hua, J., Toward a more balanced model: the revision of anti-circumvention rules, *Journal of the Copyright Society of the U.S.A.*, Spring 2013, 327-362.

13. Iannella, R., Digital Rights Management (DRM) Architectures. *D-Lib Magazine,* volume 7 number 6, June 2001.
14. Jonker, W., *et al*, Digital Rights Management in Consumer Electronics Products, IEEE Signal Processing Magazine, March 2004
15. Lima, F., *et al*. The economic dimension of the digital challenge: a copyright perspective. *Intellectual Property Quarterly*, 1, 2005, p 69-81.
16. Kra-Oz, T., Geoblocking and the Legality of Circumvention, Hebrew University of Jerusalem Legal Research Paper No. 15-31, 2014
17. Moohr, G. S., Defining overcriminalization through cost-benefit analysis: The example of criminal copyright laws. *American University Law Review*, February 2005, p 783-816.
18. Moshirnia, A., Giant Pink Scorpions: Fighting Piracy with Novel Digital Rights Management Technology, DePaul Journal of Art, Technology & Intellectual Property Law, Fall 2012
19. Peinado, M., et al, "Digital rights management for digital cinema", available at: http://www.petitcolas.net/fabien/publications/acmmm03-cinema.pdf, (accessed 27.5.2018)
20. Samuelson, P. Reverse-Engineering Someone Else's Software: Is it legal?, IEEE Software, January 1990, p 94.
21. Stormdale, C., The problems with DRM, Entertainment Law Review, 17(1) 2006
22. Valimaki, M., *et al*, DRM Interoperability and Intellectual Property Policy in Europe, European Intellectual Property Review, 28(11) 2006, 562-568
23. Westkamp, G. (2007). *The Implementation of Directive 2001/29/EC in the Member States, part II.* Queen Mary Intellectual Property Research Institute.

Books

24. Becker, E. et al, Digital Rights Management, Technological, Economic, Legal and Political Aspects, Germany, Springer, 2003.

Legislation

25. Berne Convention for the Protection of Literary and Artistic Works (1979)

26. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, The harmonisation of certain aspects of copyright and related rights in the information society OJ L167/10
27. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L111/16
28. H.R. 2281 — 105th Congress: Digital Millennium Copyright Act
29. Ministry of Education and Culture, F. (n.d.). Tekijänoikeuslaki, 404/1961. Retrieved 13.10.2015, from http://www.finlex.fi/en/laki/kaannokset/1961/en19610404.pdf
30. Ministry of Justice, Rikoslaki, 39/1889. Retrieved 7.3.2016 from http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf
31. Ministry of Justice, Kuluttajansuojalaki, 38/1978, Retrieved 8.4.2016 from http://finlex.fi/en/laki/kaannokset/1978/en19780038.pdf
32. World Intellectual Property Organization. (1996, 12 20). WIPO Copyright Treaty

Case law

33. California Northern District Court, 3:06-cv-02169, Spence v. Ubisoft, Inc.
34. California Northern District Court, 5:08-cv-04421-PVT, Melissa Thomas *et al* v. Electronic Arts Inc.
35. Superior Court of the State of California, BC343385, Robert Hull *et al* v. Sony BMG Music Entertainment Corp *et al*.
36. The Finnish Supreme Court, KKO:2010:47

Websites

37. Sarah Jacobsson Purewal, so you're being sued for piracy http://www.pcworld.com/article/230515/So_Youre_Being_Sued_for_Piracy.html (accessed 29.2.2016)
38. Andy, Received a Piracy Letter? UK Solicitor will defend you for free, https://torrentfreak.com/received-a-piracy-letter-uk-solicitor-will-defend-you-for-free-150320/ (accessed 29.2.2016)
39. http://www.turre.com/turre-neuvottelija/ (accessed 29.2.2016)

40. https://www.gog.com/support/website_help/what_is_gog_com (accessed 18.3.2016)
41. Nate Anderson, It's official: Ubisoft dumps StarForce, http://arstechnica.com/uncategorized/2006/04/6603-2/ (accessed 8.4.2016)
42. Nathan Ingraham, EA disabling 'non-critical' features and adding more servers to address ongoing 'SimCity' connection issues, http://www.theverge.com/2013/3/7/4074878/ea-deploying-more-simcity-servers-to-stem-persistent-connection (accessed 9.4.)
43. Valve S.a.r.l., Steam Subscriber Agreement, http://store.steampowered.com/subscriber_agreement/ (accessed 14.4.2016)
44. William Usher, Blizzard Faces Legal Indictments From France, Germany Over Diablo 3, http://www.cinemablend.com/games/Blizzard-Faces-Legal-Indictments-From-France-Germany-Over-Diablo-3-43626.html (accessed 8.4.2016)
45. World Intellectual Property Organization, Video Games, http://www.wipo.int/copyright/en/activities/video_games.html (accessed 10.4.2016)