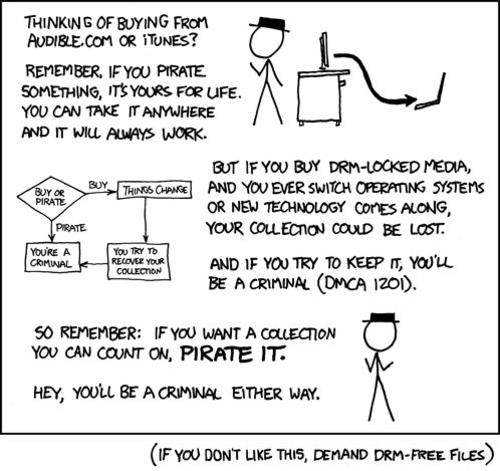
PIRACY AND DRM IN PC VIDEO GAMES: STRIKING A BALANCE

HOW THE PC VIDEO GAME INDUSTRY CAN WORK WITH PIRACY AND INVASIVE DRM



BY

Erwin van Eijden

GRADUATION ASSIGNMENT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF BACHELOR OF COMMUNICATION OF

THE INSTITUTE OF COMMUNICATION SYSTEMS AT THE UTRECHT UNIVERSITY OF

APPLIED SCIENCES

UTRECHT, JUNE 6, 2011

**Summary**

Piracy and DRM are both forces that impact negatively as well as positively on the video game industry. Attempting to work these two forces together is difficult, if not impossible. Piracy cannot be stopped, and DRM cannot work its way around piracy in any way. This paper attempts to find a way to connect the video game industry to the piracy groups that it opposes. This summary details what path was taken to get into this subject, whilst also outlining the main conclusions and recommendations.

Early research into this subject quickly showed potential for a communication approach, as it seemed there was little communication between piracy groups and the video game industry. However, the first parts of research mainly covered legal aspects and definitions, as to set up a background upon which any form of communication approach could be built. Additionally, setting up definitions and tracing the background of the issue took the helm in early research, leading to a delay in applying any communication model.

After some research and contact approaches, it became obvious that the video game industry was not going to be forthcoming with information or opinions regarding DRM, piracy or their personal stance on the issue. As a result, all information that was required to establish a point of view from the industry’s side became more difficult to obtain, and less easy to verify. Second-hand resources such as interviews and articles became the norm for obtaining information about the video game industry. From these interviews, the conclusion was drawn that piracy is inevitable for PC games, and that digital retail is a way forwards for the video game industry in regards to piracy.

Pirate groups, on the other hand, were much easier to approach, and more willing to share their view. Setting up a poll on their online forums proved an easy way to access the minds of the illegal user. Within weeks, the stance of the pirate groups was recorded, in regards to DRM and piracy. Asking them for solutions provided some interesting suggestions, all of which were recorded for prosperity, although not applicability. From this research the conclusion was drawn that DRM impacts negatively on the image of newly released video games.

After establishing these conclusions, common marketing and communication models were chosen to identify what problems these two groups faced. The lack of communication remained central, and communication models were chosen to provide a way between the two to come to some form of agreement. Unfortunately, due to the unique nature these two groups share, it seemed that no communication models were applicable. However, research into marketing models proved far more useful in attempting to solve the problem. The conclusion was reached that this issue should be treated as a marketing issue, and focus particularly on marketing in the digital world. The new focus helped in drawing up some marketing models, aimed at branding and digital marketing techniques. Some revisions in these models made them more relevant to the digital video game industry, and showed some promise in providing a solution. Coming to the conclusion that the old models were ill applicable led to the recommendation that new, revised models be used to approach the solution.

With new models in place, new marketing techniques and sales models came into play. Research done into viral marketing, proper digital branding and micro transaction sales models showed that, by using a new marketing approach, developers and publishers could reach a larger target audience and, in some cases, even ignore the threat of piracy altogether. The conclusion reached via this research was that there are solutions available within the marketing models. Recommendations based on this conclusion were aimed at mixing models and theories for a maximized effect.

**Dedication**

"*To those who Helped, and those who Help themselves"*

**Acknowledgement**

The author would like to acknowledge the following people:

Jos and Annemieke van Eijden

For their endless support and unwavering devotion

**Table of Contents**

**Summary**.................................................................................................................................1

**Chapter 1: Introduction** **and Problem Definition**.................................................................6

**Chapter 2: Providing Definitions**..........................................................................................8

2.1: What is Digital Rights Management (DRM)?.......................................................8

2.2: What is Piracy and “Cracking”?............................................................................9

2.3: Piracy: Spreading and Sharing..........................................................................10

**Chapter 3: Background Information**...................................................................................11

3.1: The Digital Millennium Copyright Act and the European Union Copyright Directive....................................................................................................................11

3.2: Fair Use Policy...................................................................................................11

3.3: Digital Publishing and Opposing Viewpoints......................................................12

3.4: Proposed Solutions ...........................................................................................14

**Chapter 4: Methodology**......................................................................................................16

4.1: Research Goals.................................................................................................16

4.2: Research Methodology......................................................................................17

4.3: Research Limitations and Threats.....................................................................19

**Chapter 5: Providing the Theoretical Framework**.............................................................20

5.1: Piracy as Communication Issue.........................................................................20

5.2: Recommended Communication Approach........................................................21

5.3: The Hurdles in Communication........................................................................21

**Chapter 6: Piracy in Marketing Theories**………………………………………………………22

6.1: Porter’s Five Forces…………………………………………………………………22

6.2: The Marketspace Model……………………………………………………………..25

6.3: Short Research: How Communication Affects Sales…………………………….26

6.4: Determining the Approach…………………………………………………………..28

**Table of Contents**

**Chapter 7: Brand Marketing- Beyond the Ads**..................................................................30

7.1: Influencing the Brand: Difficulties in Branding Video Games............................32

7.2: The Branding Model..........................................................................................33

7.3: Branding as Solution- Conclusions...................................................................36

**Chapter 8: Piracy as Viral Marketing**..................................................................................37

8.1: What is Viral Marketing?....................................................................................37

8.2: Piracy as Viral Marketing: New Perspectives....................................................38

8.3: Piracy as Viral Marketing: Conclusion...............................................................40

**Chapter 9: Micro Transactions**...........................................................................................41

9.1: What are Micro Transactions?...........................................................................41

9.2: Micro Transactions: The Good and the Bad......................................................43

9.3: Micro Transactions as Solution to DRM.............................................................44

9.4: The Digital Marketing Mix: 4S in Micro Transactions.........................................45

9.5: The SWOT of Micro Transactions......................................................................48

9.6: Micro Transactions: Conclusion.........................................................................51

**Chapter 10: Conclusions and Recommendations**............................................................52

10.1:Recommendation: A Switch to New Models and the Eye to Piracy.................54

10.2: Recommendation: The Eye to Piracy...............................................................55

10.3: Recommendation: Micro Transactions.............................................................56

10.4: Recommendation: Viral Piracy.........................................................................57

**Epilogue**................................................................................................................................58

**Reference Materials**.............................................................................................................59

**List of Footnotes**..................................................................................................................64

**List of Figures:**

Figure 1: Porter’s Field of Forces..............................................................................22

Figure 2: The Vicious Cycle of Piracy versus Development.....................................23

Figure 3: The Marketspace Model............................................................................25

Figure 4: The Branding Model of RCL......................................................................31

Figure 5: Branding model by Burnett Brand Consultancy.........................................33

Figure 6: A Simplified Branding Model for Video Game Brands...............................34

Figure 7: The 4P Marketing Mix................................................................................45

Figure 8: SWOT Analysis for Micro Transactions in Video Games ...........................48

Figure 9: The SWOT Plot of Micro Transactions......................................................49

**List of Tables**

Table 1: Bittorrent PC downloads.............................................................................38

**List of Appendices**

Appendix A: The Digital Millennium Copyright Act....................................................66

Appendix B: If Piracy is the Problem, Is DRM the Answer?......................................85

**Chapter 1: Introduction and Problem Definition**

The problem definition for this thesis is the dual nature of DRM as protector and offender. Its effectiveness versus piracy matched with its negative impact on users provides the main form of the problem definition, leading to research and policy question.

My policy question is: “What can be done to allow Digital Rights Management to effectively fight piracy?” This, of course, requires some knowledge on the subject first. Therefore, this leads to the main research question.

My main research question is: “What is the effectiveness of Digital Rights Management in fighting computer game piracy?”

The current situation, as portrayed by several developers and consumers, is that Digital Rights Management (DRM), the programs used to protect digital content, is not effective at best, and a hindrance to legal consumers at worst. Stories of inaccessible software, limited usability of purchased software and continuous issues with technical support all seem to point to the unstable nature of DRM as a defense mechanism. Considering that, in the meanwhile, illegal downloads come without DRM hassle for free, there is a definite problem.

And when some game developers[[1]](#footnote-1) come out to speak against DRM, when they are the ones hurt by piracy, then it would seem there is a definite problem with the management system. However, reading through this leads to an interesting question: “Why would game developers continue to use DRM?”

To answer that question, we need to delve deeper, and that is where this thesis’ research question comes in. By researching the effect of DRM methods on piracy, and taking into account empirical and qualitative research material on the matter, the overall effectiveness of DRM can be ascertained.

Of course, that does not yet end the problem. Considering that the problem remains with DRM, regardless of whether or not it is actually effective. And the main problem seems to be that there are only a few select cases in which DRM proved to be an effective defense. One of them, mentioned in a user’s blog[[2]](#footnote-2), and further collaborated in gaming e-zine Gamesradar.com[[3]](#footnote-3), mentions a game that took a total of 422 days to crack, using a specific form of DRM. This was one of the very few cases in which a game was cracked in more time than the average shelf life of a video game.

However, even in this one exception, DRM restricted user freedom.

The expectation runs that the research question will take some time to answer. After contact with several developers and publishers, no statements were issued on their stance on DRM. Therefore, this thesis will provide the developer’s side of the argument via second-hand media, such as interviews and articles.

Moving on to the policy question: “What can be done to allow DRM to effectively fight piracy?”

Since preliminary research and the problem statement both indicate that there is a certain issue with DRM, the policy question will attempt to find a way to come to an agreeable solution for both developers and consumers. This is not an easy task, since developers and publishers alike tend to resist the idea of changing DRM or removing it altogether.

This policy question cannot be answered without some research questions that need to be investigated. Whilst a lot of research questions at first focused on describing terminology or determining the background in legal terms regarding the issue, later research questions began focusing on the issue as a form of communication or marketing problem.

The first few research questions were focused largely on providing definitions and explaining concepts, to provide a clear background on the issue. Essentially, the conceptualization of the research. Questions such as “What is DRM?”, “What is Piracy?”, “What causes issues between Piracy and DRM?”, “What legal actions are there for and against DRM and Piracy?”. All of these questions address the problem of DRM and piracy, but only as legal issues or as a problem of the video game industry as a whole.

The next research questions focused more on finding out what could be used to solve the issue. Such questions as “What communication is there between piracy and the video game industry?”, “What stance does the video game industry take on DRM?”, “What do video game companies do to fight piracy?” and “Can communication be helpful in solving the issue?” all passed by and were answered in one form or another. As conclusions were drawn in regards to these questions, the final few questions arose, this time taking on a marketing perspective.

The research questions near the end began resolving issues and trying new models. “What can branding do for the video game industry?”, “Is Piracy a viable viral marketing platform?”, “What can micro transactions offer as a solution?” and “What models are relevant for this issue?” are all research questions that defined the final parts of this paper.

The interest in this particular subject comes from personal and interpersonal experience from the author, who is a hobbyist in the PC video gaming area. Its relevance in modern society lies in both its digital nature and its communicational issue with piracy groups and the video game industry. It shares this problem with other digital media, such as MP3’s, movies and E-books, but takes on a rather unique form due to its dual-sided nature with DRM and customer interaction with aforementioned DRM.

**Chapter 2: Providing Definitions**

This chapter will concern itself with providing definitions and explanations behind the terms and the issue that lies at the heart of this paper. After this chapter, terminology and background should be clear enough to continue into the further research.

**2.1: What is Digital Rights Management (DRM)?**

Digital Rights Management, also referred to as DRM or Digital Restriction Management, is a form of protection placed on digital files to prevent copying, downloading or spreading the files outside of legal purchases. Tracing back to the old floppy disks, DRM is an extended version of what was once basic copyright protection, which employs a third-party program to restrict use of a product.

Most forms of DRM work on a three-level management scheme:

* Establishing copyright for content
* Managing the distribution of said content
* Controlling what users can do with the content

In establishing copyright, DRM ensures that content of disks, DVD’s or Blu-ray disks are safe from being copied. The information on these disks is locked, and cannot be extracted by conventional methods. This spills over into the management of content. The actual information on the disks is accessible only by the producer. Legal consumers have no access to it, and illegal downloads have no access to the content. This prevents consumers from copying and re-selling the content.

This, in turn, leads to controlling the users’ actions in regards to the content. Legal purchasers can make use of the disk as they normally would, by watching the movie or listening to the CD. However, they cannot access the information stored on the disk. DRM seeks to make it impossible to copy the content onto any other platform than the disk and its intended player (DVD/ Blu-ray player).

Essentially, DRM seeks to eliminate the user doing anything outside of the intended use of the product. This includes copying the content, spreading it onto disks or making it available for download or purchase. Originally constructed to prevent video and music copying, DRM is currently a large trend in the video game industry.

DRM is different from standard copyright protection, insofar as that it actively hinders any attempt to copy the files for extended use. As an example, a common video may be protected by law to prevent copying, but DRM is active in a program on the video, which prevents certain hardware from reading or decrypting the information. This prevents users who want to copy the video illegally, but also hinders those who purchases the video and want to create backups for safety.

In the video game industry, DRM has become a controversial topic. DRM has always had proponents and opponents, but nowhere does this seem to be as outspoken as in the video game community. DRM on video games often limits installations of software and require online authentication of purchase. Whilst these methods scare off some illegal downloads, they also hinder legal customers with limitations in use of their purchase.

Publishing companies such as Ubisoft and Electronic Arts (both of which function as both developer and publisher in many cases) have been very active in adding DRM in their products in the last few years, much to the disarray of DRM-cautious consumers.

**2.2: What is Piracy and “Cracking”?**

(Digital) Piracy is the act of illegal downloading of software that otherwise falls within copyright protection. Essentially, it is the act of illegally acquiring software, be it via peer-to-peer networks or centralized data servers offering the software. Within the video game industry, piracy is regarded as theft, or loss of a (potential) sale. Piracy also tends to entail the “Cracking” community.

“Cracking” is a term used to describe the bypassing of protections on software, including video games, films and music CD’s. Via these cracks, users who would otherwise be blocked from the content of the disk, be it due to copyright protections or due to illegal acquisition, can readily access the content. These cracks also often remove DRM, or else seek to limit its functionality.

The two terms are commonly used together, because they are mutually dependent. Piracy relies on cracks to allow the illegally downloaded files to be used correctly, whilst crackers rely on piracy to spread the software to their audience. Due to this relationship, a lot of cracking communities function as a form of developers as well. They take the software, edit the files and then publish it to retailers or publishers, which in this case consists of torrent websites or peer-to-peer websites.

Note that between the two terms, a certain distinction can be made. Piracy is, at its core, illegal, since there is little precedent for legally providing software for free. Very few situations would call for providing software for free as the legal answer. The only exception to this is the Fair Use Policy, which is a policy set up to dictate a user’s rights within a network or between retailer and consumer. The Fair Use Policy will be detailed later.

Cracking, unlike piracy, can be legal at its core. Basic video game cracks often remove the need for a disk to be present by skipping a basic command. A lot of modern video game developers essentially incorporate this function into their games straight away, since there is no legal way of preventing consumers to crack the game to run without a disk.

Another example of legal cracking exists within the “Modding” community. “Modding” (Modifying) a game uses game files already present to create new content within the game. A common example is Counter-Strike, a game based on the popular Half-Life game engine. Originally starting out as a modification of the game to allow multi-player battle, it quickly became popular enough to spawn its own game, and subsequent sequels.

A variety of countries have declared “Cracking” legal in some ways, arguing that, once a consumer has purchased a game, he or she should have access to the game files and free reign to edit them, provided that it is then not re-sold, as that would be copyright infringement (re-selling of game files). Several European countries, including Spain and Italy, do not legally punish consumers who crack their games or video game consoles. They also allow the use of so-called “Mod-chips”, which are chips with pre-loaded modification on them, which can be inserted and installed in certain video game consoles to allow them to play cracked versions of games.

**2.3: Piracy: Spreading and Sharing**

For the purpose of this research, it is important to make a distinction between (at least) two forms of piracy. One being the small-scale “Sharing” piracy and the other being the large-scale “Spreading” piracy. These two terms are needed to evaluate which of the two influences the negative and positive aspects of piracy.

Shared piracy is:

* One-on-one, or slightly larger. Essentially, only one user has obtained the content, be it legal or illegal, and is now spreading it to a small circle of friends or relations.
* Not technically illegal. If the content is purchased legally, then copied with no aim on profit, there is no illegality (depending on the manner of content copying)
* A form of viral marketing, albeit costly. Good content may persuade illegal users to switch to a legal version. Especially is there is additional use to the legal version.
* Unstoppable. As long as content is provided legally, someone can get to it and copy the data. Bearing down on each individual case would cost more than ignoring it.

Meanwhile, Spreading piracy is:

* Large-scale, with as many as thousands of users on some of the more known websites and sources.
* A grey area of law. Content is never spread for profit, nor do many of these sites require memberships or payment for downloading.
* A chance to mass-market goods, albeit a risky one. Bad games will fade away, forever set to be downloaded. Good games will find massive numbers of pirates, but may also lead to an increase in sales of the legal version, especially if the legal version adds a significant extra.
* Technically stoppable, but very hard to do. Not all content hosted is illegal, and forcing specific files away can take a lot of time, whilst re-uploading them would happen within a time span of weeks .

Similarities between these two forms of piracy can be found via this list. They both cover a grey area of the law, and they are both hard to stop completely. Indeed, some DRM proponents claim their only use for DRM is preventing “Shared” piracy by making it harder to access legal content.

Another similarity is the idea that both forms of piracy can work as a trial version, but only on one condition: the legal version needs to have some form of “Extra” to it in order to be more appealing than the illegal version. For many games these days, that extra would be multi-player possibilities. Since many games require online presence and verification, a lot of cracked versions often work only when disconnected from the internet. As a result, multi-player is often disabled on the illegal versions, which may lead fans of the game to purchase a legal version to play online with human opponents.

**Chapter 3: Background Information**

This chapter will provide some additional background information, not necessarily related to the research question, but which are of importance to the issue at hand nonetheless. Some legal issues are discussed, as well as the digital nature of this issue, and why that digital nature is so important to the reaearch.

**3.1: The Digital Millennium Copyright Act and the European Union Copyright Directive**

When discussing Piracy, one cannot avoid the mention of the Digital Millennium Copyright Act (DMCA), or its European counterpart, the European Union Copyright Directive (EUCD). Both of these are legal directives aimed at limiting the legality of piracy, whilst also placing a certain amount of power with the consumers, rather than with the publishers.

Passed in 1998, the DMCA has been edited ever since to adapt to changing technologies and the inventiveness of pirates. Its latest revision came in 2010, and included some interesting exceptions. For this research, the most interesting one is the exception of illegal downloading for testing or correcting security flaws. In defense of piracy, this could be used to either test DRM methods, or testing whether or not a video game works on specific computer setups. However, the active spreading of this software is still illegal.

From the DMCA (1998):

*“Section 103 of the DMCA adds a new chapter 12 to Title 17 of the U.S. Code.*

*New section 1201 implements the obligation to provide adequate and effective*

*protection against circumvention of technological measures used by copyright owners*

*to protect their works.”*

This section refers to developers’ obligation to provide defenses against piracy and cracks. However, this obligation is not enforced by law, as a “No Mandate” section quickly following up on the subject points out. The obligation is aimed more at consumers and publishers, as they are the ones who suffer from the circumvention of these defenses. Consumers by paying for what could be free, and publishers for losing possible revenue due to a lack of defense altogether.

The EUCD covers the same rules as the DMCA, aside from a few sections that refer to the rights of Internet Service Providers, which are of little interest to this particular research. Likewise, the several named exceptions for circumventing technology used to restrict access are not relevant to this paper.

**3.2: Fair Use Policy**

Also known as Acceptable Use Policy, this term refers to the use of a digital network for legal purposes in otherwise illegal situations. To properly clarify, an example should be given:

If a student were to download a software program that provides information on a particular subject or allows actions to assist in the study of his or her choice, then this software falls to Fair Use; use for non-profit and educational actions. However, should this student copy the software and sell it to other students, it becomes a crime.

Fair use is often incorporated into networks or databases, in which specific rules or terms of use are described. These are widely varied, depending on the organization and type of network. However, these policies often do include the warning that any non-legal download or spreading of software will be punished. Users are told to stay within the confines of the law when using the network

**3.3: Digital Publishing and Opposing Viewpoints**

In examining piracy, DRM and video games, it is important to acknowledge that there are sources available for the legal consumer that wants a digital version. Digital retailers have been increasing in popularity. Companies such as Valve, which owns the Steam distribution platform, have been seeing an increase in users for a few years now, reaching 30 million users in 2010 and growing ever since.

Interestingly enough, Valve CEO Gabe Newell stated in an online interview[[4]](#footnote-4) on Youtube (2010) that piracy is never their main concern, providing rationalization in the following quote (Paraphrased):

*“We don’t believe piracy is a big deal. You often hear people say “Piracy means people can’t pay for a game”, but if you can imagine someone paying a thousand dollars for a PC, and for monthly internet fees, I don’t think that’s the problem. I think that you should just provide good games and good distribution. You have these companies that don’t localize their games in, say, Russia, because they say “Oh, it’ll get pirated anyway”, and then the pirates actually localize the game very well and they complain that they didn’t get sales because the pirates spread their game.”*

Newell is not alone in his thoughts. Game developer Blizzard also stated that working on anti-piracy measures is a lost cause, and that companies are better off making better games than trying to improve the protection on these games[[5]](#footnote-5).

Even Ubisoft, known and occasionally loathed for their DRM-loaded games have some praise for the way Valve deals with piracy. In an interview in the “PC Gamer Magazine” Ubisoft’s spokesman reacted to a question about Steam and their anti-DRM stance with: *“We think what Steam has done is amazingly valid, but aren’t Steam games cracked amazingly fast? It’s not a question of dissatisfaction, it’s a question of ‘we’ve got another idea, another way of implementing it, and we’re going for it’.”[[6]](#footnote-6)*

Although refusing to cooperate with this research, Ubisoft remains an important player in discovering the “Why” behind intensive DRM. Interviews with their spokesman seem to hint that Ubisoft does not really believe in the effectiveness of DRM in preventing piracy, but rather in its effect in increasing initial sales. Especially the quote in PC Gamer regarding the eventual fate of all games (to be cracked): “*They accept that it’s all DRM’s fate to be eventually hacked, explaining that internally, they’ve already talked of a timescale for how long their games will be protected by it.” (PC Gamer, 2010)*

Determining the effectiveness of DRM protection is easier within the confines of digital distribution. Because the physical aspect of business is removed, what is left is essentially legalized downloading; the polar opposite of piracy. Via online distribution platforms such as Steam, it is easier to track down illegal versions, and this may lead to a better insight into the “Why” of illegal downloading. Gabe Newell mentioned this briefly, stating that:

“*When one of our games gets downloaded illegally, we don’t see it as a lost sale. Instead, we want to see what causes people to download illegally, instead of purchasing the game.”* (Newell, G., 2009, paraphrased)

The difference we see between the reactions of Ubisoft and Valve are quite useful in determining what the video game industry is currently doing to combat piracy, if indeed they take any action at all. These two examples work well because the two companies are essentially opposite one another in their points of view, yet maintain a common stance on the matter.

Both companies believe that piracy cannot be stopped, prevented or fought against effectively. Both companies have also explained their reasoning as to the (lack of) protection they create. Valve believes bad service is the main reason behind piracy, and Ubisoft believes piracy is essentially an unchanging factor that will always influence the industry.

And both of these viewpoints lead to different approaches regarding piracy. Valve takes a passive stance, instead focusing on providing a good service and hoping that their service will attract legal customers and deter pirates.

Ubisoft takes an active stance, not believing that service is the issue, but rather that piracy is inevitable. So, instead of providing an easier service, Ubisoft provides a more difficult service with high protection measures, focusing on shelf-life[[7]](#footnote-7) rather than total protection.

Interestingly enough, Ubisoft and Valve do work together. Some of Ubisoft’s games are being sold via the Steam platform, including the DRM protection. However, since Valve, Steam and Ubisoft are all separate companies, there is no actual co-operation. Steam merely acts as a digital retailer for Ubisoft, and has no direct influence over the software that is offered to them.

The relevance between digital distribution and piracy is, according to some blog writers and videogame journalists, the ease of use. Before digital distribution, piracy was the only way to obtain a digital version of a video game, that could be used freely and could serve as a back-up. With the rise of online platforms such as Steam, the “Laziness” factor was removed from the reasoning for piracy.

In conclusion, it seems that digital distribution is one way to help combat piracy, although it still does not prevent it. Additionally, DRM is still enforced on the digitally acquired versions of the games, and so the motivation to pirate them is still present. Nonetheless, the insights offered by the spokesmen of major video game companies help determine the effectiveness of DRM versus piracy.

**3.4: Proposed Solutions**

The following is a short compendium of solutions, having come forth from brainstorming sessions regarding this issue. Whilst aiding in locating the problem and attempting to fix it, these solutions are not fool-proof and merely serve to illustrate the facets of the issue.

**Solution 1:** *Add DRM to illegal (Digital) versions, sell legal versions DRM-free*

On one hand, this solution would make illegal downloading a lot more difficult, due to the circumvention of DRM that is required to download a game illegally. It would also lower the cost of legal versions, since they no longer need to have DRM programs, which cuts licensing costs. Advertising as DRM-free may also attract more consumers, and can be used as a promotional aid. Finally, it could help with tempting illegal users to purchase the legal, DRM-less version, thus acting as a marketing tool.

On the other hand, without protection, copying legal versions becomes a breeze, which could effectively nullify all points above. In addition to that, adding DRM to the versions which are going to be downloaded illegally is a waste of money and time. In the end, this solution would hinder Spreading piracy, promote Sharing piracy, and stop neither one.

**Solution 2:** *Lower the price of games to 10-20 Euro’s or Dollars*

By lowering the price, sales of a game will rise, as per the elasticity of entertainment products, which is a benefit in itself. This solution also removes a common complaint and reason behind piracy: expensive products, or lack of funds. Furthermore, it might make consumers more accepting of Downloadable Content (DLC), since the original game is a lot cheaper.

On the downsides of this solution lies the issue that it does not stop piracy. It takes away a reason not to pirate, but it does nothing to stop it. The other two common causes of piracy (Theft and need for a Demonstration version) are still there. Additionally, to increase profit, developers might turn games into vehicles for DLC, neglecting their product. Finally, there is a threat in this solution that concerns low sales. Less sales on cheaper games means a larger loss in profit.

**Solution 3:** *Remove DRM completely*

Removing DRM as a protection means that games are no longer restricted, and no longer invade a user's privacy in an attempt to protect them. It could lower the price of games, since licensing costs for DRM are no longer incorporated. In terms of image, this could send a positive image of transparency towards costumers.

Obviously, however, removing DRM would make piracy extremely easy, which is likely to lead to reduced sales, and thereby reduced profits. It would also open up the game files, which means that modifying these files and re-using them becomes much easier. This, combined with the ease of pirating, could lead to an explosion in re-sellers, taking away sales from the developers.

**Solution 4:** *Create Draconic DRM (for absolute protection)*

By creating DRM that goes above and beyond the needs for protection, games would be protected for a longer time. It could take weeks to months to crack the code, during which the game cannot be downloaded illegally. Coupled with sufficient marketing hype, this could create a burst of sales at the release of the game, which would lead to increased profits. Finally, the powerful protection of DRM such as this would show a technical aptitude and send a message to crackers and pirates.

However, high protection would definitely come at the expense of legal consumers. Their freedom and use of the product will be limited, which will hurt the image of the game developer. Secondly, due to the ambitious nature of cracking communities, any strong security is a challenge to overcome, and draconic DRM would attract a lot of attention from these cracking communities. In addition to the threat towards image and security, the price of a highly protected game would be higher. The combination of limited freedom and increased price would make legal purchase unattractive.

**Proposed Solutions: Conclusion**

The solutions that were mentioned all showed advantages and disadvantages. The issue with all of these solutions lie in finding the correct approach to minimize the disadvantages and strengthen its advantages. Keeping in mind the number of groups that each solution should appeal to, it becomes increasingly difficult to select one method and implement it. Damaging profits, image or security are threats that are to be taken seriously, and which are quite relevant.

However, these solutions do present a very interesting image. Not one solution is effective in stopping piracy completely, which is an interesting conclusion to this research. Additionally, the proposed solutions show that DRM could be effective, when managed in a specific way. The advantages and disadvantages of each solution show that management of image, external communication and branding could all be very powerful tools in reaching a solution.

The limitations of these solutions were all based on how deeply into legal territory this issue extends. Attempting to get any form of tampering with game files declared illegal might be a solution, but it would not fit into the communication and marketing aspect of this paper. Likewise, the idea of punishing piracy or cracking as a way to deter illegal downloading was also not mentioned, due to the shift towards legal issues, rather than communication issues.

Finally, these solutions show that there are ways to handle this issue, and to handle it correctly. Whilst not providing a definitive solution or recommendation, the combination of these proposed solutions with research into communication and marketing tools could very well lead to a solution which satisfies developers, publishers, legal and illegal consumers.

**Chapter 4: Methodology**

The methodology behind this paper will explain what the research was aiming to answer, as well as the methods, or the approach, that was taken in searching for the answer. It includes the research goals, its methods, and its limitations and threats. After this chapter, it should be clear how this paper approached the issue and what it sought to research.

**4.1: Research Goals**

The research for this paper seeks to find out whether or not DRM is required to protect video game developers and publishers from piracy. At the same time, the research attempts to find a solution or alternative to the current situation which, by all means, should satisfy both the video game industry and its users, including illegal users.

The eventual solution will attempt to create an holistic image of the current situation, and apply a series of models and theories upon that image. Utilizing this method, the best solution can be picked and recommended for implementation.

To realize this, the research will set the following goals:

* To understand the viewpoints of pirate groups and the video game industry
* To research into the possibilities of using communication tools to assist in providing a solution
* Determining DRM effectiveness and impact, both on sales and image
* Adapting models to the digital world to assess their use
* Contrasting the conclusions of the research to bring forth recommendations aimed at video game publishers and developers

The first part of the research goals ties in with the research questions regarding piracy and DRM as communicational partners with dysfunctional communication. Research into their opinions and stance on the matter should provide a reasonable basis upon which communication tools can be applied for possible solutions. Additionally, it will provide some insight into the nature of the subject at large, which will be useful for the rest of the research.

Determining the effectiveness of DRM is essential to understanding the main research question, and hopes to answer it as soon as possible. Whether this can be achieved is uncertain, but a preliminary answer can always be adapted later to better suit the final conclusions and recommendations. Additionally, determining its effect on the image of a company suits itself well to set up a communication plan.

Old communication models often focus too much on the “Live” world, rather than the digital world. In an industry where many sales are made digitally, and indeed, the entire issue is considered digital, these models are usually outdated and not applicable. Revising them to better suit the needs of this paper is a research goal based on digital research and articles regarding these traditional models.

The final research goals is based less on actual research and more on performed research. By combining conclusions of earlier research, some recommendations should be made possible that provide adequate solutions, although it must be said that there is no expectation of an ironclad solution to the entire issue.

**4.2 Research Methodology**

**Phase 1: Information Extraction**

During this phase, the most important thing was to set up basic definitions and obtain information from piracy groups, developers and publishers. In order to do so, the following actions were taken:

* Approach publishers/ developers directly, in attempt to speak to PR or similar employee to obtain point of view from companies regarding DRM and piracy.
* Approach piracy groups founder(s) with similar questions, to contrast with companies’ view.
* Set up a poll on piracy forums to obtain the consumer’s views on the matter (repeated process)

To expand on the poll:

* The poll will measure the reaction of piracy group(s) towards DRM. Hypothesis states that this will be negative.
* Personal involvement in the poll will serve to extract more information where required.
* Addendum: Personal involvement will not attempt to influence answers in any way, to remain objective in gathering data.

The entire process is done online. This is partially due to the nature of the issue at hand (being the video game industry is a digital one) and partially due to personal constraints. Additionally, a lack of written books on the subject (most books focus on DRM in e-books or applications) makes literary research unnecessarily difficult.

After this phase, enough information should be obtained to form conclusions regarding the DRM and piracy issues. This would allow phase 2 to start.

**Phase 2: Contrast and Compare**

With the information gathered and the points of view of the two groups clearly considered, the research will focus on comparing the two groups. This is done to establish points of interest; be they clashes, conflicts or similarities. Via these points, it would be possible to set up conclusions that could be made relevant in communication and marketing models. During this phase, use will be made of gaming websites, game journalists' interviews and articles and scientific articles regarding the issue.

The other act in this phase is to compare the conclusions that were made to known models in communication and marketing. Finding out whether this is a problem that has a problem-solving model already is the key in this phase. If applicable, then applying this model to the case at hand and exploring its possibilities are the next step. If they are not applicable, then it becomes essential to adapt or, if necessary, create new models to apply to this case. Phase 3 will deal with this in-depth.

**Phase 3: Exploration**

With the number of models available in communication and marketing, it should be possible to find one that can be used in this situation. In that case, this model will need to be adapted to the digital world and the video game industry.

This phase is entirely focused on exploring models and ideas. Possible solutions are aplenty, which is why this phase will focus on using all previous research and conclusions to examine models, adapt them where necessary, and attempt to view their strengths and weaknesses in order to evaluate their possible use as a solution to the issue.

At the end of this phase, several options, models and theories will have been explored. Adaption of these models should allow a solution to come forth that solves the issue of piracy and the issue of DRM in one go. The next phase will then be based on the recommendation of this solution and some more information surrounding the solution.

**Phase 4: Cutting and Pasting**

Essentially the final phase, the main focus becomes the contrast of all previously mentioned conclusions and research. Utilizing the research done, the least favorable solutions will be cut out. These include any solutions that do not solve the issue, delay the inevitable or disadvantage either company or consumer.

What will be left after this is a set of conclusions and recommendations which, when pasted together, should provide the solution to the issue at hand. Whether this is the removal of DRM, intensifying DRM or attacking piracy will be left for the research part. As the final part of this phase, the video game industry should be able to take the recommendations to heart and utilize them to form a new plan to combat both DRM and piracy in a way.

As an addendum: After several contact attempts with publishers and developers, most notably Ubisoft, Electronic Arts and Valve, I received very little to no answers. All sources denoting developer’s and publisher’s stance on piracy and DRM is to be taken from second-hand sources, including interviews and articles provided by gaming journalists and websites.

On the other hand, the piracy group(s) that were contacted were willing to provide reasoning and explanation behind their actions. Therefore, with use of both primary and second-hand resources, the viewpoint of piracy groups is recorded with more certainty. Any illusion of bias or preconception surrounding this paper is caused by the lack of assistance provided by the video game industry’s big players.

**4.3: Research Limitations and Threats**

When researching the gaming industry, there are some limitations which must be made personally, and some which are created by the circumstances of the research. In the case of this paper, one limitation regarding the research came from the author. That limitation was the research into Piracy versus DRM on the Personal Computer (PC) as video game platform. This meant that all research into video game consoles (such as the Xbox 360, Playstation 3 or Wii) would not be included. The reason behind this limitation is the prevalence of piracy on the PC platform, as well as the issue of DRM mostly affecting PC games and gamers.

Another limitation to this paper and its research comes from the online nature of the research itself. Due to a combination of circumstances, virtually all research was done online. This was done, in part, due to the lack of literature regarding the subject, as well as the limited time the author could spend on literary research.

When researching online, there is always the threat of incomplete or uncertain information. Fact-checking also becomes more difficult, as there is little literature to compare the online sources to. Additionally, online research, especially on a modern subject, falls threat to becoming obsolete fairly quickly, without editing to the new situation. An extra threat in online research was the usage of online forums to obtain data. Whilst these forums are usually fairly easy in generating response, there is no feedback and no guarantee of correct answers from respondents.

Research was also limited by the digital nature of the chosen subject. Being an online industry, for the most part, the video game industry does not combine well with the traditional marketing and communication models, which are largely focused on physical products or services. Therefore, the threat of using old models to a new industry could lead to incorrect interpretation and false conclusions.

Despite multiple attempts to get into contact with some of the video game industry's big companies, such as Valve, Electronic Arts and Ubisoft, there was no possibility of receiving their feedback on the issue. Unfortunately, this created a gap in the research were first-hand material could be derived from. The choice to use second-hand materials such as interviews, articles and press releases was made to make an attempt at substituting their involvement, and to record their views.

**Chapter 5: Providing the Theoretical Framework**

Drawing from several works regarding communication within the video game industry, as well as observations of second-hand resources such as interviews and journalistic articles, this chapter seeks to provide a theoretical framework on which additional research can be built. Due to the nature of this research, the theoretical framework will focus mainly on treating the issue of piracy as a communication issue. Using the work of, among others, de Peuter, G., et al(2003) and Amoni A. (2002) et al to form a consistent image of online marketing and communication.

Personal responses taken from piracy websites and groups will be used, and contrasted with press statements and interviews with publishers and developers. Via these resources, a rough image can be drawn regarding the communication between these two groups, and how it might be improved. Models for improvement will follow in subsequent chapters.

**5.1: Piracy as Communication Issue**

Piracy is, generally, regarded as an economic issue, or a legal one. The image that many would think of when hearing of illegal downloads is that of theft, or of rebellious intention. However, this theoretical framework is interested in the viewpoints of companies and piracy groups towards one another. To get insight into these points of view, two interviews with spokesmen of video game developers[[8]](#footnote-8) and publishers[[9]](#footnote-9) will be used, alongside the opinions of piracy groups, recorded from an online poll.

From the aforementioned interviews come the interesting observation that piracy is fought on one hand, and ignored on the other. Gabe Newell, CEO of Valve, actually states that “*At any time, Piracy is way down on our list of issues… often as low as number nine”* (Paraphrased). Meanwhile, a Ubisoft spokesman stated that *“It (Piracy) is a huge problem. You know it, I know it…”* (Edwards, T., 2010). However, it is interesting to see that both parties do not mention communication with piracy groups.

Observations taken from an online poll on a piracy group’s website[[10]](#footnote-10), along with a number of other forums, seem to confirm the lack of communication between piracy groups and the video game companies. Further online research also shows no apparent links between piracy and video game developers or publishers, aside from legal issues and law suits.

In conclusion, the theoretical framework of this paper is convinced of a lack of communication between piracy groups and the video game industry. This sets the theoretical foundation for research into marketing and communication models to attempt to find a solution.

**5.2: Recommended Communication Approach**

Communication is a very broad understanding, and as such, merely mentioning that it forms the problem between two groups is no guarantee for success. The theoretical framework will require a specific form of approach towards communication to build further research on. Unfortunately, very little research is done on this subject, due to its digital nature, combined with its difficulties in assessing communication success on online platforms.

Due to the lack of research, the framework will instead rely on informed conjuncture, based on the author’s personal experience with communication failures in online environments, as well as a communication and marketing education background.

In any online situation, extended communication is always required. The next part of the theoretical framework will deal with this in some detail.

The recommendations this paper will eventually provide are aimed at the video game industry, which means that all research has to be based on its advantages and disadvantages for both groups, but with the focus on the video game industry, including developers and publishers.

**5.3: The Hurdles in Online Communication**

Communication online is a difficult subject. The limited means to express a message, combined with the endless amounts of information that can be found online create a pressure, and that pressure creates difficulties. The “Hurdles” in communication differ from subject to subject and issue to issue. However, a short introduction to online communication, provided by the Spin Project[[11]](#footnote-11), serves as a useful guideline to overcoming these hurdles.

However, one additional problem within this paper is the involvement of DRM. When asked about their opinion towards DRM, many users of a piracy group website responded negatively, with very few remaining neutral on the issue. An anonymous board also responded with great hostility towards any mention of DRM. As a result, online communications can be hindered by DRM methods.

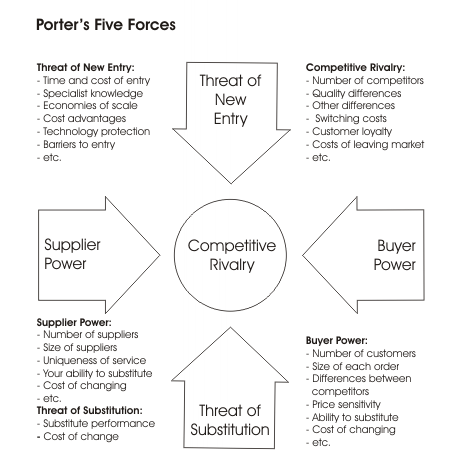
The biggest issue in overcoming the hurdles of online communication, especially between piracy groups and the video game industry, is to connect the two groups, whilst trying to keep the negative attitude created by DRM out of the way. The theoretical Framework builds on this, and any research done on this issue is to be connected to both groups and DRM, to see whether a solution is possible that pleases every group.

**Chapter 6: Piracy in Marketing Theories**

Because this paper seeks to treat piracy not as a legal issue, but as a communication and marketing issue, it is vital to understand what role piracy takes in common marketing theories and, indeed, to see whether marketing theories apply to piracy in the video game industry at all. Analyzing common marketing theories and models, and adapting them where possible is the eventual aim of this chapter.

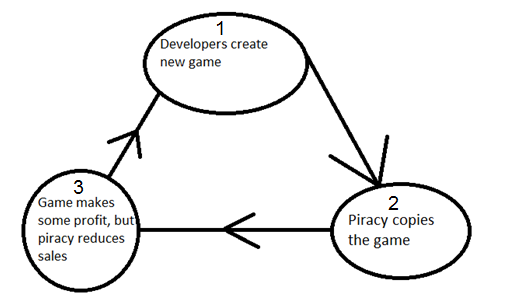
**6.1: Porter’s Five Forces:**

Due to the rather unique position that piracy takes in the video game industry, it would be helpful to place it in a common model. I have chosen Porter’s Field of Forces (Figure 1) because piracy is an external force, hovering in between consumer and thief, with both being adequate descriptions. Porter’s Field of Forces seemed the most logical choice to me, because it deals with the balance of power in business situations. As such, the balance can dictate on the use of DRM.

* Figure 1*: *Field of Forces, Porter, 1979, (taken from mindtools.com)*

Neither suppliers or New Entries are of importance in discussing piracy, and will therefore be ignored. Our main focus should be on “Buyer Power” and “Threat of Substitution”. Piracy hovers in between these two forces, being both a substitute (in providing the same product, for free), yet comprised of Buyers (pirates being consumers still, and acting like regular customers.)

The first hurdle is the Threat of Substitution. In a very real way, the two main points of substitution (performance and price) are very much present in piracy. Not only is the same product delivered, but often it is done so with better service (cracks/ mods). Additionally, piracy offers the product for free, which is a price no publisher or developer could match.

And yet, at the same time, the only way the substitute can be this effective in the first place is by the developers of the game. Since piracy works only as a copy machine, it does not create its own products, leaving it in the hands of game developers to consistently bring forth new products. The cycle is shown in Figure 2, demonstrating the connection.

*Figure 2: The Vicious Cycle of Piracy versus Development (van Eijden, E., 2011)*

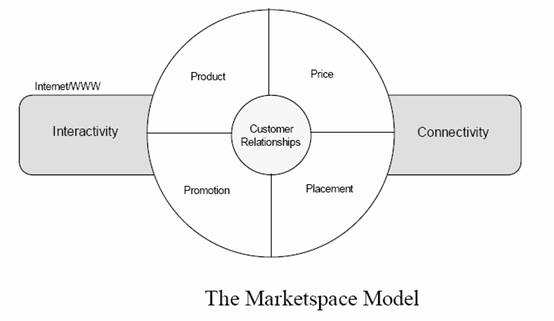
However, figure 2 is only an assumption. We can be sure of step 1 and 2, since developers bring forth their game, and piracy will copy it. However, we cannot successfully determine whether a game makes profit, or whether it loses sales over piracy. If it does, then piracy is the negative influence in this figure. However, if piracy does not decrease sales, or even improves the sales figures due to word-of-mouth marketing, then piracy acts as a marketing tool.

Deciphering the relationship between piracy and game developers is a difficult task. No answers are set in stone, and plenty of case studies show equal effectiveness on both sides. Perhaps the hardest thing to deal with in the case of piracy is the struggle to compete with one’s own product. The equivalent would be to have two identical cars being sold, one with the backing of a manufacturing company for a set price, and the other for free, without the developing company’s backup.

Competing with an own product means that company image, reputation and customer loyalty all become more important. Since any form of tarnish on the image or reputation may drive loyal customers to the free, illegal competitor, keeping up with your customers becomes a priority. This is where DRM comes in. Since restrictive DRM is not uncommon among many games, it begins to annoy loyal customers. Restricted access, limited possibility to work with provided content and increasingly paranoid verification checks all hurt the image of a fun hobby.

Invasive DRM leads to piracy, as can be effectively proven via examples. To avoid constant verification checks, cracks have been invented, which often come from pirate websites. To bypass the limitation on installations, illegal versions of software often come with unlimited access to installations. To allow access to content, piracy decrypts and spreads digital content that would otherwise be inaccessible. However, piracy is not just illegal software (or, for the sake of this research, it is not.) In today’s digital world, illegal copies of video games serve as demonstration versions of the game. If a game proves to be a good game, then the chances rise of the game being recommended to the pirate’s friends, co-workers or other relations. In essence, downloaded versions can work as trial versions, inciting sales for good games and acting as a form of viral or word-of-mouth marketing.

**6.2: The Marketspace Model**

If piracy can indeed be considered an image issue, in which a company has to compete with itself, then the logical answer would be to study some image branding concepts. De Meyer, et al 2001 and Amoni, et al, 2000, created the Marketspace Model (Figure 3:)

*Fig.3: Marketspace model by Amoni, 2000*

In this model, two important sidelines are given to determine the market model. “Interactivity”, as stated by Amoni (2000) *“… Has to do with two-way exchange of information and ideas with the customer through an on-line interface”*, which means that companies connect to their users (Leading to “Connectivity”) via forums and online presence.

The 4 P’s are still present, but now they all encompass a single goal: customer relationships. From a shift in perspective, companies in the digital world have had to adapt to the increasing strength of the demands of the consumer. The DRM issues seem a clear Product/ Placement mishap, leading to botched Customer Relations. Meanwhile, piracy is clear, open and willing to communicate (interactivity), whilst providing the same Product, for the lowest Price, making use of the company’s own Promotion and Placement.

This model leads us to one possible conclusion: That video game developers and publishers are actively hindering themselves and promoting piracy via DRM. Their Promotion goes to waste, their Prices are too high, their Positioning is only getting worse in the Customer’s eyes and their Product is being given away for free.

A lack of interactivity between the companies and publishers seems key here. And where some companies openly embrace the opportunity, such as Valve, others remain painfully distant and quiet. Unwillingness to communicate via interactivity is regarded as an unwillingness to speak to customers. Modern companies, and especially such companies that produce digital wares, should move with the time.

**6.3: Short research: How communication affects sales**

To indicate the use of communication to increase sales, or at least attempt to convert pirates to legal purchase, a short research into the success of proper marketing and communication could sway companies to a different viewpoint than pure economic reasoning.

A modern example for video game marketing methods is the Gears of War 3 campaign, running a three-part advertisement for the game on consoles and PC. “Your Brand is Showing”, a blog on marketing and communication, mentioned the perfect brand name alignment that Gears of War offered to its target group. Using the Thunderbird marketing program, essentially stating 5 requirements for proper marketing, categorized as:

* Category Need
* Brand Awareness
* Brand Attitude
* Brand Purchase Intention
* Brand Purchase Facilitation

In this model, the campaigns for Gears of War scored very high on Category Need (the current development of hyper-realistic and violent games), and added Brand Awareness on it, based on the popularity of Gears of War 1 and 2, which were both considered (paraphrased from game journalist review:) “Over-the-top gorefests with hyper-violent tendencies” ("Your brand is Showing" Blog, 2010). Building on that image, the campaign released three videos that showed lots of violence, blood and realistic environment.[[12]](#footnote-12)

Effectively combining the first three parts, marketing for Gears of War 3 proved highly successful, with sales reaching 12 million in 2010. Proper reaction to the image of their game made this advertisement all the more effective.

However, this is loosely connected so far. How, then, can this model be brought into play for communication towards pirates? Research done by the Simon Fraser University (Burnaby B.C., 1998) showed that proper communication towards video game consumers follows slightly different lines than the messages required to reach other audiences. It is essential, according to their research, to maintain a constant outlook on the industry at large.

In analyzing the Thunderbird marketing program, the two obvious points for video game piracy are Brand Attitude and Brand Purchase Intention. For physical wares, Brand Attitude (BrAtt) eventually resolves into Brand Purchase Intention (BPI). However, for video game companies, there is a line to be drawn within BrAtt, in order to divide the “Would Download” consumers and the “Would Purchase” consumers. This means that BrAtt is essential for eventual purchase.

Additionally, BPI becomes a different threshold for video games; a higher point to be reached than in the original model. Since purchase involves actual support towards the developer, it becomes more important than Brand Purchase Facilitation, especially since digital distribution has become more commonplace. So, the new model would limit itself, but also add onto the old. An adapted Thunderbird model would look like:

* Category Need: Research into the market to see whether demand for a video game is sufficient to release a new title.
* Brand Awareness: Previous releases in the series, or games made by the developers, can add to Brand Awareness, which leads to a better Brand Attitude.
* Brand Attitude to Purchase Intention: The position that the consumer takes on the developer, and their subsequent intention towards the product. This combined point can be split into three categories:
* **Aware, no interest:** These consumers are aware of the product, but not interested. Additional marketing and communication might peak them up to higher levels of interest
* **Interested, would download**: These consumers would download the game illegally, or for a very low price. Their interest and awareness are raised, but they are not (yet) willing to pay full price.
* **Interested, would buy**: These consumers are aware, interested and motivated to purchase. They are willing to support the developers financially, via legal download or purchase

Brand Purchase Facilitation is now worth it to be put on the list; games can be downloaded easily, legally or illegally. Secondly, many big companies will have their game readily available in regular stores as well. In the case of video games, brand purchase intention is linked directly to attitude, rather than facilitation.

What does this mean, then, to video game companies? Basically, it means that Brand Attitude is everything. And whilst Brand Attitude can be influenced via pricing, it is much easier to do so via correct marketing and communication. It also provides a twofold bonus: not only does this allow pricing to be much the same, but consumers are lured from two different perspectives; piracy groups and unaware groups. Whereas lower pricing tends to simply raise sales by a set amount (for example: lowering the price on game X by 50% leads to a 50% increase in sales), proper brand marketing could essentially boost sales whilst also building on a positive image for companies.

**6.4: Determining the Approach**

Now that there is a fairly stable analysis of the problem at hand, it is time to focus on possible solutions. Before anything is suggested, however, it is important to determine what angle should be taken to tackle this issue. For this, some old research and articles will be used to figure out exactly what can be done to assist the video game industry.

First off, this problem will be approached as a Communication and Marketing issue. This is mainly in relation to Valve’s stance on piracy, combined with Ubisoft’s idea on piracy. Whereas Valve sees bad service as an incentive to pirate, Ubisoft believes that customer dissatisfaction is irrelevant to the equation of piracy.

Secondly, in examining the market forces that video game companies face, piracy has been identified as a unique force: a competitor that offers the same products, with less service but at no cost. As a result, bad service seems the main differentiation between legal and illegal games. The financial aspect may be of influence, but as was mentioned in an interview with Newell: Pirates have spent hundreds or thousands of dollars on their PC’s and internet connections. It is unlikely that they cannot afford to purchase a game.

Finally, we have seen that piracy is an unstoppable force. DRM may provide a wall to run into, but it cannot stop piracy. At most, it can delay the inevitable long enough for a game to outlive its shelf life, which seems to be Ubisoft’s idea of “Effective” DRM. And yet still, the cost for this form of protection comes at a loss to service and satisfaction, as demonstrated by forum complaints and research done among video game pirates.

Combining these conclusions, the approach that seems most valid here is to communicate with the pirates, and provide better service. How to improve services will be an important aspect of the solution. Winning back the loyalty of pirates that have so long been used to free games at the click of a button will be the most challenging part. Unlike most business sectors, the video game industry is filled with competitors that give away copies of products for free; not exactly a common problem in say, the Automobile industry.

To analyze this approach properly, a quick look at the pros and cons it offers should allow a more holistic view on the issue:

Pros:

* Closest connection to the issue
* Target group is reached relatively easily
* Offers opportunities
* Shows transparency, willingness to communicate
* Multitude of possibilities in communicating
* Group is already aware of the issue

Cons:

* Negative image might make communication seem hostile
* Resources used on “Thieves” might be considered wasted
* Target group is easy to reach, hard to reason with
* Position of pirates hard to determine; methods of communication unclear
* Threat of averse or negligible effect

Most of the cons can be remedied via good communication, and mainly with the right message. However, since piracy is in such a unique position on the market (being both competition and consumer, at entirely different levels), the threat of miscommunication and the amount of resources required can be daunting for many companies. If companies take this approach, then they need to be informed of the possible rewards.

Mainly, then, the information they seek needs to be formulated in a “Better than” format. Economically speaking, video games have a rather high elasticity. Essentially, the more a video game costs, the less it sells. As a luxury product, or entertainment product, video games also tend to be swayed by the economic market when changes occur (although the recent crisis had affected the video game industry less than other markets), leading to reduced sales on high-priced games, but relatively stable sales for low-price games across the board. With an eye on this elasticity, would decreasing the price be an easier solution than communication to pirates?

**Chapter 7: Brand Marketing- Beyond the Ads**

*“A brand for a company is like a reputation for a person. You earn reputation by trying to do hard things well.” -* **Jeff Bezos**

Brand Marketing is defined by the American Marketing Association as:

*“ (A brand is) a customer experience represented by a collection of images and ideas; often, it refers to a symbol such as a name, logo, slogan, and design scheme. Brand recognition and other reactions are created by the accumulation of experiences with the specific product or service, both directly relating to its use, and through the influence of advertising, design, and media commentary.”* –Source: American Marketing Association, 2010 (referencing SEMPO)

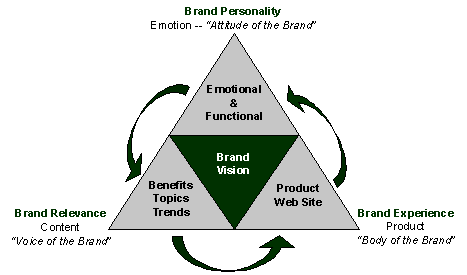
In simple terms, Branding is the reputation, or accumulated experience, with a brand or company. Brand Marketing is essentially brand improvement or management, and is known as both Branding, Brand Marketing or Brand management. Minor differences in definition state that Branding is a start-up of a new brand or overhaul of an old one, whilst Brand Marketing is raising awareness for a brand via positive reinforcement of brand values. Brand Management is considered an everyday underlying process on which companies operate; everything that a company does can be considered a piece of brand management, even more so when it later gets reported in the media. (Based on definitions from the AMA, 1995-2011)

The mention of Brand Marketing is relevant to the research into DRM versus piracy. Especially the mention of “…*The accumulation of experiences with the specific product or service”* is highly indicative of the form that DRM has taken. From negative experiences with the product (not functioning due to DRM production or limited in usability) to the service that lies behind these products.

Especially modern video games, which often contain a multiplayer mode online, are very conducive to bad performance on service and product. The online aspect is essentially a service; hosted on the servers of the developer and provided for consumers. The product contains this service, and with purchase comes the unwritten promise that this service is maintained and available. DRM often makes this service unavailable to legit players without identification (CD keys or login codes), or contains errors which bar access to the content from legit players.

Previous research into DRM has shown that it has notoriety among consumers, with many opponents to the protective measures, and very few proponents to defend it. This was most likely the cause for a decrease in trust and a tarnished image and reputation for many game developers who sought to protect their product via DRM.

The Research Center Ltd. Made a basic branding model in 2006, concerning media branding. Considering the messages and form in which video games are spread, they are considered media, and as such fall within the purview of this model.



*Fig. 4 : The Branding model of RCL, 2006*

Brand Vision encompasses the brand’s idea of what they are. For example, Coca-Cola has the brand vision of “Sharing Happiness”, and its functionality, its emotional message and its corporate messages all envision this. Unfortunately, video game developers and publishers often suffer diminished visions, due to the number of games they release, each of which counts as its own brand name.

In “The Interaction of Technology, Culture, and Marketing”, De Peuter (et al., 2003) mentions the difficulties in determining solid brand vision for video games. The wide nature of video game genres, combined with the publishing companies’ front-line personality (developers often take on the publisher’s role, too) make it hard to determine what Brand Vision a company should take, if any at all. Considering that each new and original game requires a new vision, a new plan of action and a new target group, it is nearly impossible to create one vision in which developers could place their games.

Nonetheless, there are some things that we can take from the RCL model. Naturally, a Brand Personality can always be established in a detached form (with no relation to the games being sold.) Provided publishers and developers can shape their messages and focus on providing solid service with appropriate media support when required. The functionality that is mentioned in this model can be considered compromised by DRM. Restrictive DRM also provides a company with a new face, or attitude; in a negative light.

Brand Relevance is perhaps the easiest part to conform to with video games. Trends and topics in video games generally follow a basic line (categorized in genres), and these allow for variation in non-radical ways, which means that expansion within the genre can easily be done to match current trends and topics (for instance: Shooting games in which the Taliban represent the enemies.)

Brand experience is tainted, as was mentioned before, by DRM. If the product places restrictions on its use, then it will negatively impact the image of the brand. The Brand experience is the “Body” of the brand. In this case, this entails both the digital product (the game) and its additional services, which overlap with the Brand personality (like online functionality). Since DRM cuts into these services, it becomes a handicap with which companies have to work with.

**7.1: Influencing the Brand: Difficulties in Branding Games**

Kadayifcioglu (2009) made a short compilation of the difficulties in properly branding video games. As was mentioned earlier, the fact that each game represents a brand means that only single-genre developers are “Suitable” for branding. As an example, Kadayifcioglu names Bioware, which is a American-owned Canadian game developer. For years, Bioware stuck to the genre of Role-playing games, and made a number of critically acclaimed titles, and to this day Bioware is often mentioned when asked for a “Solid” game developer brand.

However, aside from exceptions such as Bioware, most game developers spread their franchises over different genres. The danger in focusing on one franchise or title is stagnation of that franchise, especially when publishers demand new titles. An example of this is mentioned by Barton (2007), who names the Ultima franchise after its take-over. Pressured by publishers to produce new titles, Ultima VII, VIII and IX were released, with content cut from the final product.

Publisher branding is easier, especially for those publishing companies that focus on single genres, or have affiliated themselves exclusively with a game developer. It becomes difficult, however, when the developers also publishes its own games. Electronic Arts has four different labels with which they promote their games, and each one focuses itself on specific genres of video games they develop.

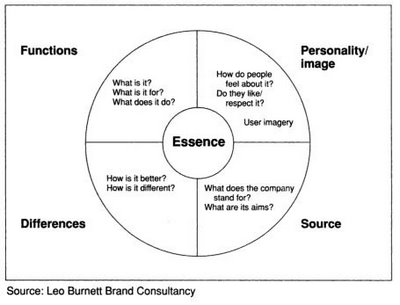
The difficulty with branding in video games lies primarily on the holistic attributed that branding possesses. A brand is a collection of experiences, past and present, as well as the promise that a brand holds. And whilst that makes sense for a company like Coca-Cola, which produces one product and delivers it well, it is much harder for video game developers, who often produce a range of very different experiences. Of course, there are messages which span the width of the gaming experience (Electronic Arts’ “It’s in the Game”, for instance), but these are uncommon and very general.

How, then, can branding be influenced within the video game industry? Especially when focusing on what DRM does to the brand image of video game developers and publishers, it seems that proper branding could really promote legal purchases. Why, then, is DRM still rampant, and are there still developers that include highly invasive anti-piracy measures with their product?

Previously, the conclusions were made that piracy figures are often exaggerated, that the influence of piracy can assist as well as harm sales, piracy cannot be stopped and DRM has an overall negative image about it. All of these points would seem to support the removal of DRM from video games completely. And whilst some developers do, indeed, promote their game’s “DRM-Free”[[13]](#footnote-13) approach, an equally large amount still uses such DRM methods as SecuROM, or even more heavy protection software.

**7.2: The Branding Model**

Figure 5 depicts the common branding model, developed by the Burnett Brand Consultancy. Unfortunately, this model is relatively old (1997) and as such is not entirely usable for this particular case, since it is based on the "Traditional" form of branding, in which face-to-face contact and physical products are the most common branding facets. However, we can take the basics and set up a new model via combination of branding models, in order to shape this model for the digital world, aligning it with the digital world the research works with.



*Fig. 5:Branding model by Burnett Brand Consultancy, 1997*

Key terms within branding, which constantly resurface, are:

* Functionality
* Emotion/ Feeling
* Vision

Functionality entails the service or product that is being delivered to the customer, quality-wise. For the video game industry, this means the software to install, the game, and its additional content (where available). Proper functionality is restricted via DRM and other protective measures that block gameplay.

Emotion, or feeling, is the joy that a consumer gains from playing a game. This is more than just the instant gratification as experienced by the user. It also factors in the immersion into the game’s world, and the universe in which the player is transported when playing. A common example of Emotion done right could be a highly atmospheric game (Amnesia: Dark Descent), or it could contain a depth in its game world that makes the player part of the world (World of Warcraft.)

Vision consists of the developer’s and the publisher’s view on what the game’s brand should be. It is the basic premise upon which Functionality and Emotion are built. Proper vision guides development of games, leading to correct functionality. When the vision also focuses on protection, and DRM specifically, its knowledge of the target group could possibly present a form of DRM that is, at least, agreeable to the consumer. Essentially, the vision behind a game shapes everything about it.

So, for every game that is developed and published, a new brand is created. Setting up a simple three- part model would result in a model like figure 6.

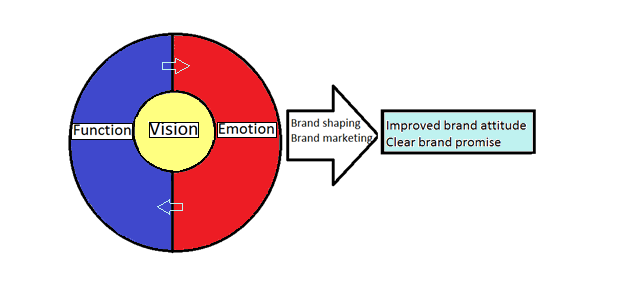
*Figure 6: A simplified branding model for video game brands (Van Eijden, E., 2011)*

Figure 6 shows that Vision lies at the core of game design (as with most brand designs). During the vision shaping process, all decisions regarding the brand should be decided upon. Inclusion of DRM is also decided upon within the vision. Surrounding Vision are Function and Emotion. These two parts together create Vision, whilst Vision is the basis for the two others.

Function is defined as “Delivering on the promise”. The promise in this case being the vision. Essentially, the vision of a game is its quality, its genre, and its content (or gameplay). Additionally, in this process of shaping the brand the form of DRM (if applicable) is decided upon (common DRM forms such as SecuROM, for instance). The Function is part of a circle with Emotion.

Emotion comes with Function in a singular circle, and is defined as "The Experience or Feeling". These two parts influence each other, since a proper Function leads to a better perceived Emotion. Emotion, in this model, indicates the feeling, or connection, that a user creates with a particular brand game. Vision guides what this feeling should be, and Function guides how it is communicated.

This model can be used to brand a video game based on its three most solid aspects: Its ability to influence the users, its fundamental function and the promise it offers prospective customers. Utilizing these three correctly leads to a shaped brand, which is easier to find a market for.

DRM methods are an important part throughout the process. During the vision part, it is important to understand what the video game brand should feel, do and act like. This also includes DRM, especially since the overall view of DRM is negative (refer to poll at Piratebay and other gaming sites[[14]](#footnote-14)), which means that inclusion is likely to reduce positive attitude towards the brand.

During the Function part of branding, the decision to use a specific form of DRM is taken. Additionally, if the brand is to send a certain message, Function decides on how to send that message. Additionally, if a video game brand is to use Downloadable Content, then Function decides what is in this extra content, as well as what protection there is for users to download and/ or install the content.

The Emotion part of branding is focused on how users experience the brand. In the case of video game brands, this starts at purchase and installation, and requires extra attention towards DRM methods and how they are enacted. Previous examples of DRM gone wrong (such as the Ubisoft case) should provide plenty of example on how to use DRM the wrong way. The important idea behind this model is that DRM should be modeled towards the vision and its eventual users.

Using this model correctly should “Shape” the brand. A brand that is properly shaped has several advantages, such as:

* Name recognition
* Clear communication goals
* Clear definition of function
* Proper desired brand image

Of course, there are also downsides to this model. It does not, for instance, focus on external forces or threats. The entire model is based on the idea that a concept can be visualized and then given form via a simple model. It also skips over additional steps in creating Function and Emotion. Additionally, this model does not deal with piracy or protection against piracy, aside from its decision to implement DRM or not, made during the Vision and Function decisions.

The model is also limited, in that it generalizes the entire video game industry in a single model. Not all video game brands can make use of this model to its full extent, since some games have no focus on Emotion, or purposely wish to limit Emotion or Function in exchange for other forces. This model also limits itself to the creation of image, and not to its maintenance or continued appeal.

**7.3: Branding as Solution: Conclusion**

All of these aforementioned advantages created by Branding help in marketing the video game brand, since they make it easier to set up marketing campaigns and commercials. Additionally, Function should make the brand more desirable for users, since proper gameplay and content is set up during the Function part.

The main issue with this approach lies within its effectiveness. This approach does not seek to eliminate DRM, or even attempt to change its current effects. It only hopes to reduce its negative image via communication measures. When effective, this method could potentially reduce piracy rates, but there is no guarantee on its efficiency.

Eventually, the branding model should improve brand attitude, or provide a clear brand image in case of a new and original video game brand concept. In case of existing brands, this model can be used to ascertain the brand’s promise. Whilst not the best solution, this model can at least find some use in branding video games.

Looking at the downsides and limitations of this model, it can also be concluded that this model's only use is for setting up a new video game brand. It does not help existing brands, nor does it seek to provide maintained usability for a brand. It also runs the risk of being forced out by other brands, or by external forces which are not mentioned in the branding model itself.

**Chapter 8: Piracy as Viral Marketing**

This chapter seeks to explore the option of using piracy as a form of viral marketing. Earlier mention of this has been made, but not properly explored. This chapter will clarify what viral marketing is, what it requires and how it might be of assistance to video game developers who want to utilize communication and marketing as a solution to piracy.

**8.1: What is Viral Marketing?**

*“One theme [of viral marketing] will likely recur: originality. Originality that draws on popular culture or is so brilliant that it becomes popular culture.” –* Haas, C., 2010

The above quote by Christian Haas is essential in understanding viral marketing, a practice which is described by the American Marketing Association as:

*“A marketing phenomenon that facilitates and encourages people to pass along a marketing message. Nicknamed viral because the number of people exposed to a message mimics the process of passing a virus or disease from one person to another” –* American Marketing Association, 2011

Earlier in this research, a short mention was made of using piracy as a form of viral marketing; a sort of word-of-mouth advertising via the illegal spreading of video game software. This segment hopes to find an answer to the question: Could piracy be used as a form of viral marketing?

First off, it is important to understand the pitfalls of viral marketing. Writer, M. (n.d.) wrote a short article on disadvantages of viral marketing. A short review of these disadvantages and how (or if) they relate to the video game industry:

1. Usually unsustainable: Viral marketing is hard to keep up, since it requires new content to be pumped around the desired networks.
2. Loss of Control: Once spread, you cannot influence viral marketing.
3. Threat of “Fad”: Extremely short-lived viral marketing fizzles out and leaves a bad impression

1a. Moderately Relevant: Video games are constantly in production, and pirate websites continue to spread them. Additional content is not hard to produce, and will be spread around the networks easily. The threat here may lie with the abundance of content, rather than the lack of it.

2a. Highly relevant: There is absolutely no control over what happens to a video game that spreads illegally. Even worse is when a game is spread before the final version is released, and contains errors or severe lack of content. Illegal players could act as bad advertisers for the final product!

3a. Relevant: The threat of fizzling out shortly after release is highly possible, especially in a market with as many products and brands as the video game industry. However, the chance of leaving a bad impression is reduced, provided the quality of the game is deemed to be of reasonable standard.

Aside from disadvantages, however, there are also positive sides to viral marketing. Scott, D.M. (2008) mentions some of these in his own, (highly viral) article on viral marketing. Among some of these advantages, the most relevant are:

* World-wide audience due to the internet approach
* Low-cost marketing (note: less applicable in video game industry)
* Reach larger audiences
* High possible gain with little input

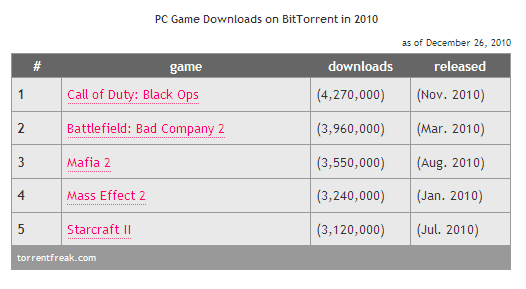
**8.2: Piracy as Viral Marketing: New Perspectives**

When talking about the video game industry, it is impossible to ignore the effect that the internet has had on marketing video game brands. Although very few figures exist for video game companies pre-internet era, it is a likely assumption that their sales were a lot lower and their marketing a lot slower.

Looking at the advantages and disadvantages of viral marketing and comparing them to the piracy situation that has been discussed earlier leads to a few points of interest.

The first point of interest is that Piracy seems to be a form of viral marketing already. From personal experience, as well as collected data from personal environment via interviews with fellow video game hobbyists, forum visits (such as 4chan: /v/, 2011 and Gamefaqs, 2011) and personal correspondence within social circle, many video games that were illegally downloaded and proved to be of good entertainment value were bought at some later point, and recommended to friends and family. Of course, this is only on a small scale, but all viral marketing starts out small.

However, looking at the numbers as depicted in figure 7, and compared to the sales figures of the games mentioned in figure 7, piracy amounts to almost 75% of the sales of a triple-A title such as Call of Duty, which sold 5.6 million copies.



*Table 1: PC downloads from Bittorent in 2010, provided by* [*www.torrentfreak.com*](http://www.torrentfreak.com)

It is wrong to assume, however, that these are all lost sales, or even sales at all. Though only old figures are available (2004), the reasoning behind piracy usually stands at around 20-25% for two to three main reasons, these being:

* Try before buy (potential customers) – roughly 25%
* It’s free (no lost sale/ 50% chance of purchase)- roughly 20%
* Would buy, download instead (lost sale)- roughly 15%

*(Figures taken from Assorted websites, including Piratebay (2011), PC Gamer (2010), Gamasutra (2010) and personal experiences and correspondence (2011) )*

Now, if we look at these figures from another perspective, we see that roughly four million potential customers downloaded the game. This also means there was a capacity of four million possible viral marketing points. With this in mind, the conclusion that the five million sales figure might have been assisted by a form of viral marketing is not too difficult to believe.

But the previous example was an unintentional form of viral marketing. Very few gaming companies have ever decided to release a full version of their game for free in the hopes that this would attract paying customers to the product. And, indeed, the very idea seems wrong. Since video games are not physical products, such as skin cream, they are not as easily given away in “Sample packages”. And giving customers total access to the final product for free is not a profitable move.

How, then, can viral marketing be made accessible to the video game industry? This is a pretty difficult question, and one without a ready answer. Already, most video game developers are, in a way, active in viral marketing via illegal downloads. They just are not aware of the fact that these pirates might be helping them in promoting their product. This leads to a different suggestion.

What if video game developers and publishers could find a way to acknowledge piracy as a viral marketing campaign? This would not be too hard; most companies are aware of their game being spread via illegal downloads, and most of them also realize that there is no way to prevent these downloads from happening. And, when faced with a neigh-unstoppable force, why not try to use it in a positive way?

Steinberg (2010) stated that perhaps, the way forwards for the video game industry, is to simply release full games for free (or severely reduced) price, and adding additional content via in-game payments (or micro transactions) to increase revenue, rather than selling a game up front for 50 to 60 dollars.

However, research into the subject has already shown that this is not a favored way forward by consumers. An anonymous research had shown that many customers prefer not being “Nickle-and-dimed” by developers, feeling that even optional payments infringe upon their free use of the game. The most notable case in this matter is Valve’s Team Fortress 2; a one-purchase game which, in 2010, received an in-game item shop, where game items could be purchased with real money. Shortly after the addition of the shop, the community board of the game was filled with complaints and praise for the cash shop system.

If the video game industry could acknowledge the viral marketing possibilities of piracy, then it could deal away with DRM completely. However, with no research done into the matter, chances are that removing DRM and releasing games at the mercy of piracy could lead to greatly reduced sales. Lack of research on the matter makes any venture into piracy as viral marketing tool very dangerous, especially if the idea should fail.

**8.3: Piracy as Viral Marketing: Conclusion**

In conclusion, piracy is already a form of viral marketing; it just is not acknowledged as such by the video game industry. Proper acknowledgement of this fact could lead to guide piracy into the marketing business as a high-risk, high-reward tool. This could probably be done via different branding, or setting a new vision in which piracy is incorporated as an additional force.

With the potential to carry viral marketing messages, as well as the ability to provide additional content easily, video games can become very important marketing tools for the video game brand or its developer’s brand. Micro transactions could be used to replace the cost of otherwise illegally downloaded games, but these pose a risk to brand image.

The biggest threat for video games remains the fact that piracy offers the same product for free, and that adding anything onto the product for purchase might seem like an attempt to get more money out of legal customers, rather than an attempt to get illegal users to spend money on the product.

**Chapter 9: Micro Transactions**

Exploring additional payment options is the main focus in this chapter. In an attempt to see whether changing systems and perspective might help combat piracy, this chapter researches the payment model known as micropayments or micro transactions. Naturally, the nature of micro transactions will be explained, as well as what needs to be changed for micro transactions to work properly.

This chapter further expands itself with a new take on the Marketing Mix and a SWOT analysis, with plot, for the micro transaction payment method. These tools are used to determine the eventual use that this method might hold for the video game industry.

**9.1: What are micro transactions?**

In the Viral Marketing chapter, a brief mention was made of micro transactions within video games. Essentially, this would allow video games to become the retailer of products, and the main source of profit for the game. This alternative solution could become a worthwhile choice, which is why this chapter will focus on using micro transactions as a way to reduce prices and motivate purchase.

Whilst there is no real video game specific definition of micro transactions, the most commonly used definition (taken from the Collins English Dictionary/ the Free Dictionary):

“*A system whereby a user pays a small fee to access a certain area or part of a website.”* (Collins Dictionary, 2003)

A slight change should be made for this definition to be more relevant to the video game industry. It would then read as follows:

“*A system whereby a user pays a small fee to access additional content in a video game.”*

The origins of this practice trace back to a text-based online game called “*Achaea, Dreams of Divine Lands”*, released in 1997 by Iron Realms Entertainment. After some time, in-game auctions were held, in which special in-game items or services could be bought. Although originally meant to be a one-time occurrence (as was stated by Mihaly, M., CEO of Iron Realms Entertainment[[15]](#footnote-15)), it soon became a regular part of the game. This led to a new phenomenon where the game itself was provided for free, but additional content could be purchased via in-game stores for real money.

This system of micro transactions or micropayments has become increasingly popular in Massive Multiplayer Online Games (MMO’s). While the list of completely free online games shortens, the list of initially free games with cash shop option lengthens. To name only five MMO’s with a cash shop:

* Allods online
* Lord of the Ring online
* ACE online
* Cabal online
* Dungeons and Dragons online

The most interesting of the above named games is Lord of the Rings online (or LoTRo). Originally released as a subscription-based game (akin to World of Warcraft, where a monthly fee is required to keep playing), it changed to a free game with cash shop in 2010. Since then, the developers have claimed a threefold increase in profit in comparison to their old subscription-based system[[16]](#footnote-16). Of course, this change was not without complaints, and indeed, a portion of consumers expressed their indignation at the ability to purchase what they have been working for all that time.

Despite complaints, however, the results are undeniably profitable. Tripling the profit that the company was making prior to the introduction of the cash shop is no small feat, and it shows that consumers are willing to pay for additional content, especially when other parts of the game are still provided for free.

Not only Massive Multiplayer Online games are influenced by micro transactions, however (although it is the predominant leader in the area). In September, 2010, Valve added a cash shop to Team Fortress 2, one of their top-selling games. Via this cash shop users could buy cosmetic changes to their characters, as well as other content, that could previously only be gained by playing the game and obtaining a set few achievements.

Although no figures have been released by Valve yet, the store can only be running a profit. The original game is often on sale on Steam, sometimes for as little as $2.50. The cash shop, on the other hand, has additional content available for prices running up as high as $50,00. And whilst it is completely optional to purchase anything from the item store, there are still plenty of users who are willing to spend extra money for digital content.

**9.2: Micro transactions: The good and the bad**

The advantages of micro transactions are obvious, though for consistency, they will be listed here, along with disadvantages, aided by the work of Yonzon, Y. (2008):

* Low cost to create
* Easy to incorporate in game
* High reward, low risk
* User retention based
* Providing the game for free nullifies piracy risks
* Free games need no DRM

The idea of a low-risk, high-reward system of selling content appeals to many developers, but there are some disadvantages to be considered. These are mainly focused on Brand Perception; the way consumers view a brand. The disadvantages are:

* Forced upon users
* Creates a “Nickel-and-Dimed” feeling among users
* Unbalances gameplay (influences Brand Attitude/ Emotion)
* Laziness risks
* Reliance on cash shop for profit is risky

To elaborate upon these points:

Users often feel that cash shops are forced upon them. In the case of Lord of the Rings online, as was mentioned earlier, many users took to the game’s forums to complain about the new shop, and how it felt unfair to paying (premium) users. Likewise, Valve garnered some negative comments when first introducing their item store, mainly aimed at how it “forced” new users to purchase content from the store to keep up with regular users.

This leads to the second disadvantage; the feeling of being “Nickel-and-Dimed”, a commonly used term when describing micro transactions, which returns in complaints listed about both Lord of the Rings online and Team Fortress 2. The term refers to “small payments”, but is also a negative term that implies “Shaking down” users until they’ve spent their last nickel and dime. Cash shops often provide imbalanced content, which makes users feel the need to pay for additional content, or be disadvantaged in a way.

The additional content is often imbalanced, or runs risk of tipping balance. Especially in multiplayer games, balance is often difficult to find within gameplay, and when it is achieved, it is easily broken by releasing additional content. Nick Yee (2004) commented that online games, and especially Massive Multiplayer Games, are easily affected by seemingly small changes. And badly balanced games affect the user’s emotions and attitude towards the game (brand).

Another common problem that developers run into, especially when providing free online games, is the risk of turning lazy. This ties in with the unbalanced content, since developers who focus on profits might turn away from attempting to fix gameplay issues, and instead focus on pumping out more content to be used in micro transactions. Notable examples of this attitude are *‘Fly For Fun Online”* and *“GunZ Online”,* both of which have built up a reputation for focusing on producing more cash shop items than actual meaningful content.

Finally, the risk of putting a video game brand in the hands of micro transactions is quite substantial. The reasoning behind these small payments is, after all, that a large number of users is willing to spend money on an otherwise free game. This relies on two essential parts:

* A game with appealing content, to attract users
* Incentives to use the cash shop

These two parts work together, but also against one another. Any game which appeals on its own risks having a useless cash shop, since everything a user wants is already provided for free. Meanwhile, focusing on incentives to use the cash shop is likely to cut into game content, reducing its appeal.

**9.3: Micro transactions as solution to DRM**

In theory, using micro transactions is a valid replacement for the current business model of video games. It removes the issue of piracy almost completely; the game is given away for free, which means piracy becomes useless. Meanwhile, since no purchase is required, any form of protection can also be removed, since validation of purchase is not important.

Provided that the basis of a game is appealing enough (and, for many existing game brands, this tends to be the case), it would not be too hard to add additional content via micro transactions. Concerns for profit can be assuaged via previously mentioned examples of successful implementation of the micro transaction system.

From a communication aspect, introducing micropayments is part change management and part marketing management. Users will have to adapt to the new system, which will invariably be coupled with protests (Baekdal, 2006). This will need to be handled carefully to prevent loss of users or severe image damage. At the same time, management within the company will have to adapt their vision and way of business to the new payment methods. This also affects external communication, since stakeholders may not agree with the change in business model.

Of course, change management has to be backed up, in this case, by marketing management. Not the product, but the position of the product becomes important here. Differentiation from the common denominator is extremely important in luring new users. Fortunately, the market for online games has a very identifiable common denominator: World of Warcraft. With an estimated number of 12 million subscribers, the market’s biggest share of users can be found in World of Warcraft.

**9.4: The Digital Marketing Mix: 4S in Micro Transactions**

Traditionally, the 4P marketing mix model, as shown in figure 7, was used to determine the usability of a new model or approach in regards to marketing. It showed four points of interest upon which those models could base themselves.. However, that marketing mix was created before the advent of the internet and the creation of internet-based transactions and stores. Since this research is based on the digital world, it is better to use a new, adapted model.

*Figure 7: The 4P Marketing Mix, 1960, taken from Softducks.com*

The 4S marketing model (E. Constantinides, 2002) was created to provide companies that wished to expand their business online with a new marketing mix model. No longer utilizing the 4P model, the 4S marketing model instead focuses on a digitally managed and controlled environment in which transactions are made. Its relation to the digital video game industry and micro transactions will be made clear in this chapter. The reason for selecting this new model over the traditional model comes from the decreased effectiveness of several parts of the traditional model in the online world (such as Place and Product), which are therefore better off being replaced.

The 4S marketing model is, unfortunately, unavailable in image format without requested permission of the author (Constantinides, 2002). Due to time constraints, this paper will include the 4S model in text format instead.

The 4S model consists of the following marketing mix elements:

**Scope: Strategy and Objectives**

In which analyzing the market, customers, internal processes and the role of the online transactions within the company takes the lead. Used as a primary step, Scope will allow a company to set objectives and decide on a strategy to get the most out of their online business.

In the video game industry with micro transactions, Scope can be used to determine the competition within the game’s genre, to analyze what sort of users the game is likely to attract, what is required to introduce micro transactions into a game and what role these extra transactions will play. Utilizing this step to analyze the market will make entry into that market a more manageable step.

**Site (Store): Web Experience**

Customer-oriented content, based on determining how well the potential customer can use the internet, and how experienced the user is at navigating websites or online stores. Questions such as: “What does the customer expect in a shop/site?”, “Why will the customer make use of this shop/site” and “What motivates customers to return?” determine Site as a marketing mix element.

In the video game industry with a focus on micropayment, this step is used to set up how a potential customer uses the micropayment store, and to analyze how easy to make navigation through that store. Replacing “Place” in the 4P model, Site focuses not on *where* purchase takes place, but on *how.* Proper utilization of this step will allow companies to set up a model with which customers are familiar, which in turn allows for a smoother transition towards the new model, and more users to utilize the micropayment store.

In the video game industry specifically, this S can be replaced with “Store”.

**Synergy: Integration**

With a focus on working internet technology to real-life instances, Synergy is used to set up the network required to route the money from customers to the Site/Shop to the company. Takes on a slightly different format in the video game industry.

Within micro transactions, Synergy is mainly used to determine how the game interacts with the payment system. Visibility of the micropayment store within the game might be an aspect of Synergy. Likewise, integration with payment methods and external payment servers are part of the Synergy step.

Secondly, Synergy focuses on integrating the micro transaction model into the departments found within the company. This means that departments such as Legal and Marketing are aware of, and integrated with, the micro transaction model. This will prevent mishaps and set the company for a more attuned stance towards online transactions.

Properly executed, Synergy sets up the financial part of the micro transaction model. By combining the payment platform with a company’s bank account, and ensuring a safe payment model for potential users, Synergy is how the flow of money comes from user to company.

**System: Technology, Technical Requirements and Web Site Administration**

System is the final S in the 4S model, and focuses on the technological aspects of the marketing mix model in a digital environment. When dealing with any online-based business attempt, it is important to have a technical staff that understands what is expected of them and how to keep it running.

In the video game industry with a focus on micro transactions, the most important part is Site (Store) administration and maintenance. Ensuring that the store is online is essential for profit flow, whilst regularly offering sales or discounts via the store falls under Site administration.

Properly setting up and maintaining the System is essential to profit flow and customer satisfaction. Online businesses, and especially games, are almost required to be online and functioning 24/7, especially when their profit depends on it.

**Conclusion: 4S Marketing Mix Model**

In changing to the micro transaction model, the 4S model provides more relevant information than the traditional 4P model, and is therefore recommendable. Whilst some of the old Ps are missing, these usually have little to no actual effect on digital sales, and can therefore be missed. Some other parts of the old marketing mix have been retained in the new 4S model (Site replaces Place, for instance).

How a company decides to use the 4S marketing mix model is up to them. According to Constantinides (2002), the model is best used by following through in the order listed above, to ensure that all analysis is done by the time the integration and execution is performed. Utilizing this marketing mix model should allow a new company to enter the market prepared and without major issues.

**9.5: The SWOT of Micro Transactions**

Micro transactions are fairly new, and opportunities regarding micro transactions in video games have been ill-documented, at best. Certainly, developers have caught onto the idea that users are willing to pay small prices over, say, subscription per month or single-purchase (traditional) payment. However, what it offers over other forms of payment is usually not mentioned.

A SWOT (Strength, Weakness, Opportunities and Threat) analysis of micro transactions will provide an overview of what micropayments can offer a developer, based on the idea of reducing piracy and removing DRM; a viability research into the shift towards a new model. This SWOT is demonstrated in figure 8 and 9

Figure 8: Swot Analysis for Micro transactions in video games. Template taken from [www.businessballs.com](http://www.businessballs.com/), on May 12, 2011

**Weaknesses**

* **Service vulnerability**
* **Dependent on base (free) product**
* **Reduced piracy rates= reduced viral marketing rate**
* **Initial product forced to cut down on content**
* **Bad image**
* **Competition with many other brands**
* **Loss of piracy players**

**Strengths**

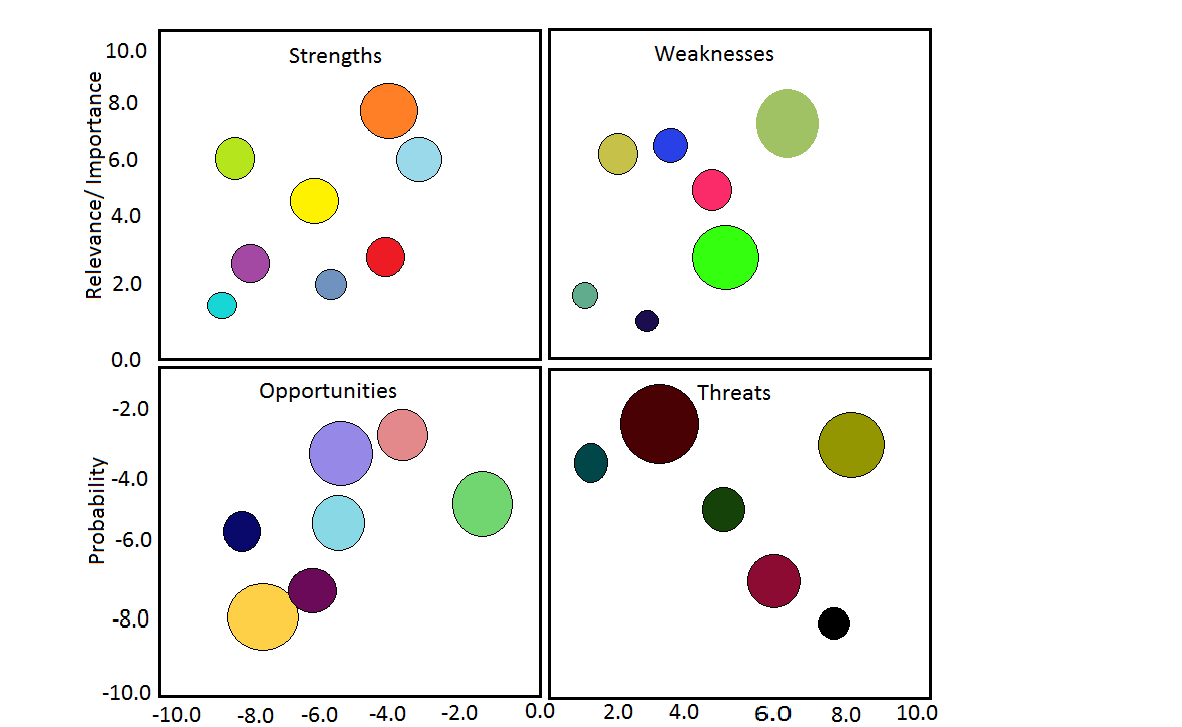
* **Reduced piracy rates**
* **Attracts a large audience via free product**
* **Retain profitability**
* **Highly adaptable prices**
* **Can always add new content**
* **Limitless profit cap**
* **Lower production time**
* **Competitive advantage over subscription or payment model**

**Threats**

* **Hacker vulnerability**
* **Difficult to “Stand out”**
* **Danger of core product changing due to additional content**
* **Insufficient hype/ buzz leading to early downfall**
* **Game becomes vehicle for content; loses appeal**
* **Lack of customer spending; customer not using micropayments**

**Opportunities**

* **Endless expansion**
* **High marketing potential**
* **Viral marketing among free users**
* **Allows for user-generated content**
* **Continuous innovation**
* **Works as testing area for new brands**
* **Does not need DRM**



*Fig.9: the SWOT Plot of Micro transactions, 2011. Underneath: Legenda*

As with all SWOT models, a lot of different parts from the model provide counterarguments to one another. Having piracy disappear also means that the potential for viral marketing is reduced. Meanwhile, the opportunity for infinite spending is offset via the threat of no spending whatsoever; this is all dependent on content, which is also mentioned as both strength and weakness. In essence, however, this analysis provides useful information regarding the use of micro transactions.

Reviewing the SWOT plot, the biggest and most relevant threat comes from hacker vulnerability; the chance that hackers could come into the system and potentially uproot the micropayment system or worse. This threat can be prevented by acting upon the weakness of Service Vulnerability, plotted as slightly irrelevant, but still potentially threatening when left unchecked.

Another big threat is the danger of turning the game into a vehicle for additional content. This ties in with the weakness of being forced to cut down on the main focus of the game, along with the weakness of dependency of the main product. If the main product does not appeal, then this threat will become reality and the game will slip down the drain until no user wishes to pay for it; they feel that they do not get the “full” experience from the start, and are thereby “forced” to pay.

Meanwhile, the biggest weakness lies in the combination of unfinished products and negative image. The opportunities for viral marketing and the promise of endlessly expanding on the original (free) product can make up for this, and it is recommended to do so. Applying strengths to opportunities to counter the weaknesses and threats is the key focus of any SWOT, and this plot should provide the necessary framework to do so.

The biggest problem with this SWOT plot is the forced importance placed on each individual issue. The SWOT parts are all important when combined with one another. Apart from each other, not one of them is actually a bigger issue than the other, but the forced importance placed on each individual aspect makes it difficult to adequately plot them. In the end, this SWOT plot is fundamentally flawed, and only marginally useful. In comparison to other notions regarding micro transactions, this SWOT and plot are insignificant.

The conclusion that can be drawn from this analysis is that micro transactions can definitely be a valid answer to the problems regarding DRM and piracy; it does theoretically contain the answers to do so. Pirates cannot download free games illegally, and the additional content should be made either hard or impossible to download without payment; an easy method when using virtual currency.

However, care must be taken in shifting from a traditional sales method towards micropayments. It requires a different form of marketing, a certain approach towards users (image marketing) and a secured transaction platform, managed independently to minimize security risks.

Additionally, since micropayments require constant online presence to be used effectively, one DRM-like issue remains. However, with a separate transaction server, this could be avoided.

**9.6: Conclusion: Micro Transactions**

As a potential answer to piracy and as a counterpoint to invasive DRM, micro transactions are a valid answer. This conclusion can be drawn from example cases (Turbine; Valve), to varying degrees of success. There is no cap on the profit, as compared to subscription-based or sale-based models, as long as the user is willing to pay.

Substantial shifts in design surrounding games would have to be made, but these are manageable. At the same time, all communication activities surrounding the game will require a make-over. Differentiating the product via marketing management will become essential to attract users. Branding and image marketing will have to instill in users the trust that micropayments will not negatively influence their experience.

The SWOT behind the micro transaction model shows that there are substantial threats, opportunities, weaknesses and strengths. However, as was mentioned in the analysis of the SWOT and the SWOT plot, these are largely connected to one another and to external circumstances, and are more a result of the weakness of a SWOT than of the micro transaction model.

The micro transaction model has a high potential for game developers, in a lot of areas. Innovation in terms of game experience, an endless profit cap and the ability to expand upon a single product or brand for a long time are all within range of the micro transaction model.

Unfortunately, in order to implement the micro transaction model, great care must be taken of the customers, since these have been proven to dislike the micro transaction model, and to develop a negative image of companies that decide to use it. Additionally, the shift to a new form of payment platform and the need to spend additional time and money on maintenance, communication and customer feedback might scare potential adapters of the micro transaction model away.

**Chapter 10: Conclusions and Recommendations**

Throughout this paper, several terms, conclusions and points of interest were pointed out and resurfaced on numerous occasions. Combining these conclusions, with particular attention paid to their strengths and weaknesses, will point out the recommended path for video game publishers and developers. These recommendations will focus largely on removing piracy as a threat and utilizing less or no invasive DRM.

First off, some interesting conclusions:

* Piracy is impossible to stop; it can only be delayed, at best
* Piracy provided the game industry with the worst form of competitor; one who can provide the same product for free
* Invasive DRM is not a good answer to piracy; it effectively harms companies and attracts pirates
* There is little to no communication between pirates and game developers or publishers
* Communication and Marketing can be used to counter the seemingly legal and economic issue of piracy
* The digital market surrounding the video game industry allows more opportunities to fight piracy

To touch on some of the important conclusions: Piracy is impossible to stop because it will always find a way through whatever protection has been set up against it. Delaying it is not recommended, and indeed it may be recommended not to attempt to stop it in the first place. Additional to this conclusion comes the fact that any strict protection is going to invite hackers, crackers and other groups to break the defenses.

DRM is no answer, as has been stated a few times in this paper. Any form of DRM is going to be considered a defense to shatter. And the harder the defense, the more challenging it is to break it. Since many hackers are young and rebellious at the core, the chance to break “The Unbreakable” is something that not many of them would pass up, if only to brag about it.

The Digital market removes one of the oldest reasons to pirate: Back-ups or digitalized versions of the game. This used to be common in the disk era, but it has become obsolete now that any game can be downloaded from a digital retailer, and can be regained from the digital retailer should its original be lost.

These are all points which have returned, in one way or another, in every approach to the issue. The image that these conclusions created is that of an overshadowing threat of piracy over the entire video game industry, unable to be stopped or prevented. The idea of piracy as an external competitor that was, essentially, too strong to compete with, led to some recommendations for an approach to the issue:

* Do not fight piracy; it cannot be stopped
* Since piracy is not fought, do not treat pirates as enemies
* Acknowledge potential in piracy in marketing and communication areas (viral marketing)
* Create a new business model, involving piracy as external force which can be influenced via internal activities

To clarify onto the previously made points for a bit: Piracy cannot be stopped because any attempt to do so only incites the pirate groups to fight back. Enforcing DRM encourages piracy to crack it, and gives them a challenge which they will gladly accept. Added to that is the fact that any protection can be cracked, eventually, thus ensuring that piracy cannot be stopped.

Treating piracy as an enemy or rival competitor is detrimental to a company's efforts. It is equivalent to competing with a company who sells the same product for free, which makes it a waste of time and money.

When piracy is no longer an enemy, it can become a market force. A volatile one, but still a useful extra. Utilizing the free products they spread, companies can adjust their marketing and communication to match the message: Get these products, and buy them if you want more. By making use of this message, companies can decide to adapt the recommendations on the next few pages.

**10.1: Recommendation: A Switch to New Models and the Eye to Piracy**

Many of the models used in modern marketing and communication areas were originally created for the traditional business model, with physical goods and stores. With the creation of online stores and digital wares, particular care has to be taken in using these models, since they often ignore weaknesses found in the online environment.

Within this paper, several models were adapted to better fit into the digital world. These new models are still not perfect representations of the same models in the traditional sense, but they can serve as starting points for companies who want to move into the digital market place.

Particular care has to be taken to apply these models, as each video game brand requires a different outlook on its intended target group, its genre and its image. Applying the models requires some market research, but has the distinctive advantage of allowing future sequel games of the same brand to be used in roughly the same way.

Traditional models have landed the video game industry into its current situation; it believed that protecting its product would stop theft, but in the digital word, theft loses its meaning. Marketing, too, makes a larger shift towards image marketing and brand attitude than in the “Real” World. Especially since piracy allows users to test out a product before purchase, which could lead to disappointment and, as a result, negative brand attitude.

The main recommendation of this paper is the shift to a free-to-play model[[17]](#footnote-17), with micropayments as primary source of profit. Compared to the other, currently available forms of payment models, this model has the longest lifetime and highest profit cap.

Another recommendation that this paper has formed is the recommendation of putting piracy in the market model; essentially incorporating piracy into the overall business plan. This means that piracy (and pirates) are to be viewed as a second market; be they testers for an early version or a gateway to viral marketing, they can be valuable to obtain data regarding the game brand.

Both of these methods stop piracy, in a way, from being an issue. In the case of micro transactions, piracy is useless, since the game itself is merely a vehicle for the additional content provided via micropayment. Downloading it illegally costs nothing, and even “Copycat”[[18]](#footnote-18) games (or private servers hosted via file leaks) will have to resort to micro transactions to pay for maintenance.

In the same way, using piracy as a way to keep tabs on the market and its consumers allows companies a modern version of “Demonstration” versions. Early releases could lead to positive feedback, or it could lead to feedback which can be incorporated in the final product. When combined with micro transactions, this method could incite enthusiasm among users before the game even hits the (digital) shelves.

This recommendation comes with the recommendation to switch perspectives when viewing and dealing with piracy, mentioned on the next page.

**10.2: Recommendation: The Eye to Piracy**

Throughout this paper, second-hand sources often find that game developers and publishers may view piracy in a very negative light, refusing to work with pirate websites and piracy groups. And yet, from a communication perspective, it is piracy which forms an important element to game developers, especially in terms of marketing research.

A very strong recommendation to provide to those companies unwilling to change models to micropayment is to monitor or include piracy groups into their communication and marketing activities. Within these activities, pirates are to be treated as potential consumers, but with one overlapping thought: These consumers are capable of obtaining and criticizing your product before actual purchase, so their feedback is essential.

Treating piracy as an additional market force, rather than as a criminal group, can lead to massively improved potential for marketing and feedback alike. Especially with such digitally present groups as pirates, it is relatively easy to obtain feedback and see where the spread ends up.

Whilst a niche group, piracy groups do show interest in the products created by the video game industry. Why else would they go through the effort to copy and distribute it? This shows that, despite appearances, this group could potentially grow into more than merely “thieves”.

Whilst incorporating piracy into market models is by no means easy, it might be useful to take a look at the “Piracy in Marketing” chapter, in which piracy is mentioned as a mixture of consumers and competitive entrants. Proper utilization of this new perspective will open up a new market, for which new models and theories can be created.

**10.3: Recommendation: Micro Transactions**

Any video game company that feels threatened by potential customers turning towards piracy can be recommended to switch to a Micro Transaction or micropayment model. This paper has taken in advantages and disadvantages of a shift towards such a model, and can readily advise a step to be taken towards it.

Keeping in mind the recommendation of switching to new models, micro transactions require a very specific form of marketing, and likely some technological changes as well. The 4S model mentioned in this paper can be of great use in determining how to implement such a model. Additionally, to maintain image towards users, the image marketing and branding advice provided should prevent a negative image swarming the decision to implement the new model.

The reasoning behind this recommendation is quite simple: Delivering a free product means that there can be no piracy (who can steal a free product[[19]](#footnote-19)?), which also means that there is less requirement for DRM that hinders or limits customers. Additionally, the fact that the video game market is moving towards the digital world means that selling additional content via micropayment becomes much easier. This model can even be integrated into the product itself.

Of course, every recommendation needs to keep in mind the impact it has on its customers. Micro transactions are, generally, regarded with suspicion. The feeling that developers create entire games and then cut content before presenting it to consumers create hostility among users who find themselves cheated out of the entire product. This can, of course, be remedied via open and honest communication, with particular mention towards branding and social media, which can be used to show users the “Behind the scenes” of micropayment models.

In the micro transaction model, service and protection will take on a larger role in the development of video games, and in their subsequent release. This will be a step forwards for the video game industry at large, since it will mean lesser games produced, but with more, and more extended service towards customers. Properly protecting the transaction platform will also require some additional work. But it will keep out piracy and DRM, and when properly dealt with, it will open up an entirely new market segment.

This recommendation will require a dynamic change in marketing, communication and branding, unless the company in question is a new entry into the market, in which case it will require a different outlook on new business than traditional models would provide. Among the important factors are branding (image marketing), content delivery and consistent communication with the users. Models within this paper can be used as guidelines towards ensuring success.

**10.4: Recommendation: Viral Piracy**

Marketing games is hard. Considering each game can consist of a different genre, and many games tend to quickly descend into copying one another, standing out as a gaming brand developers is something that requires a considerable deal of attention.

Recommending Viral Marketing to video game developers is essentially nothing more than ensuring that proper products are created, sold and, most importantly, downloaded. To add up on the previous recommendation: treating pirates as marketing tools is a way to incorporate them into the market model of developers and publishers.

In viral piracy, it is important to understand the mind of the user. Interaction via forums, websites and personal feedback could be of great assistance in ensuring that all players, including the illegal users, pass along the message that video game developers want them to. Of course, not all target groups can be reached, and the danger that this presents is that a party downloads the game and criticizes it. This is, however, always a danger, in legal and illegal downloads. The main idea is to provide an experience that players wish to share, thus ensuring viral marketing feedback.

Downloaded games often lack some components; be it online play, the ability to customize or other options. Legally purchased versions do have these features, and as such they will be interesting to those who want to experience the full package. Using piracy as a viral marketing tool, these features become selling points.

A potential downside here is that DRM is not excluded, unfortunately. However, as long as the DRM is not invasive or disruptive, and no mention of the DRM is made as a way to keep players out of content, this should be a manageable method.

**Epilogue**

As an afterword to this paper, allow me to write an epilogue, as a form of finisher or send-off, informally speaking. This paper has sought to combine piracy, DRM and the video game industry, in order to find balance between these groups who, otherwise, tend to go for the throats of the others. Whilst it may not have succeeded entirely in doing so, it has, in my personal opinion, found ways to deal with piracy and DRM from a communication and marketing perspective that is interesting to the video game industry.

Originally, my expectations were set a bit higher, with hopes of interviewing some of the big video game companies and receiving their opinion on the matter. Unfortunately, this was not to be the case, and I was forced to use online sources to establish their point of view. On the other hand, my personal experience and involvement in the video game industry as a consumer with a critical mindset did help me in establishing the sides of Piracy and the video game industry.

Large amounts of research within this paper had to be checked for relevancy and legitimacy, the obvious pitfalls of online research. My sincerest hope is that I did not skip or slip over any part of the research, especially regarding the eventual conclusions and recommendations which were based on that very research.

The eventual recommendations and conclusions in this paper are aimed at the video game industry as it stood in 2011, and may not be entirely correct for future usage. However, it is my hope that the industry takes note of this issue and finds some form of assistance in communication and marketing in order to find a way to work with piracy. I, personally, believe that to be a better solution than the endless legal battles that the industry attempts to fight and which, it seems, never seem to amount to anything.

Remember: Piracy is not necessarily an enemy. DRM is not a flawless protection method. Switching to new models of marketing and branding might be required, as it might be necessary to switch to alternative methods of promoting video games, branding video games and, in some cases, incorporating piracy as viral marketing for video games.

As a video game player, part-time pirate and part-time legal consumer, this paper might seem like a marketing tool to legal consumption to some and as an incentive to illegal downloads to others. I wished I could bring this in any other way, but I am afraid that my personal stance on the matter is the same as many others:

*"If you have to, pirate. But if you like the game, and want to see more like it, buy it. Alternatively, send sixty bucks to the developer, so they know you support them."* (van Eijden, E., 2011)

Addressing you, the reader, on a personal level for a moment: Thank you for your time and attention. I hope that my research, conclusions and recommendations, along with the setup for this research, were more pleasurable for you to read than for me to write. It is my vision that future generations of students can look back onto this paper and find some form of knowledge to obtain from it.

To that prospective student: Good luck.

And to all others who have read this: I thank you for your time and your attention.

With kind regards,

Erwin van Eijden

**Reference Materials**

**Online Articles/ Bibliography**

**Amoni A, Biren B, Dutta S** (2001):Business Transformation on the Internet 2000**,** INSEAD, available from <http://knowledge.insead.fr/docs/2001-22.pdf>, retrieved on April 5, 2011

Anonymous author, 2011, *“The Price of Microtransactions: Runes of Magic”* <http://www.mmocrunch.com/2009/08/12/the-price-of-microtransactions-runes-of-magic>, retrieved on May 2, 2011

Anonymous Author “*The World of Text MMO’s / MUDS- an Interview with Matt Mihaly, CEO of Iron Realms Entertainment”* on Play no Evil: <http://www.playnoevil.com/serendipity/index.php?/archives/765-The-World-of-text-MMOs-MUDs-An-Interview-with-Matt-Mihaly,-CEO-of-Iron-Realms-Entertainment.html> retrieved on May 2, 2011

Baekdal, T. (2006), Change Management Handbook *“Handle Change Management Projects More Effectively”* on HU Sharepoint:

[https://www.sharepoint.hu.nl/sites/ICM%20Year%204/Communication/CHAMAN/Course%20materials/Articles/Baekdal,%20T.%20%282006%29%20Change%20Management%20Handbook.%20Handle%20Change%20Management%20Projects%20More%20Effectively.pdf](https://onderwijsteams.sharepoint.hu.nl/sites/ICM%20Year%204/Communication/CHAMAN/Course%20materials/Articles/Baekdal,%20T.%20(2006)%20Change%20Management%20Handbook.%20Handle%20Change%20Management%20Projects%20More%20Effectively.pdf) , retrieved on April 29, 2011

Barton, M., 2007, *The History of Computer Role-Playing Games Part 1: The Early Years*, on Gamasutra:<http://www.gamasutra.com/view/feature/3623/the_history_of_computer_.php>, retrieved on April 19, 2011

Borden, N. H., 1964, “*The Concept of Marketing”*, Cambridge University Press, retrieved from <http://www.commerce.uct.ac.za/managementstudies/Courses/bus2010s/2007/Nicole%20Frey/Assignments/Borden,%201984_The%20concept%20of%20marketing.pdf> On May 2, 2011

Burnaby, B.C., 1998, *A report from the Media Analysis Laboratory,* Simon Fraser University. Available at <http://www.media-awareness.ca/english/resources/research_documents/reports/violence/upload/Video-Game-Culture-Leisure-and-Play-Preferences-of-B-C-Teens-Report-pdf.pdf>, retrieved on April 19, 2011

Cocoran, I., 2007, *“The Art of Digital Branding”,* published by Allworth Press, New York

Collins English Dictionary, 2003, published by HarperCollins, on <http://www.thefreedictionary.com/_/misc/HarperCollinsProducts.aspx?English>, retrieved on April 28, 2011

Constantinides, E., 2002 “*The 4S Web Marketing Model”* From Elsevier/ Electronic Commerce Research and Applications: <http://doc.utwente.nl/42661/1/4S.pdf>, retrieved on May 12, 2011

Francis, T., 2010, “We ask Gabe Newell about Piracy, DRM and Episode Three” on PC Gamer: <http://www.pcgamer.com/2010/09/15/we-ask-gabe-newell-about-piracy-drm-and-episode-three/>, retrieved April 19, 2011

Gilbert, B., 2010, *“Activision: Black Ops tops Modern Warfare 2 day-one Sales Records”* on Joystiq: <http://www.joystiq.com/2010/11/11/call-of-duty-black-ops-day-one-sales/>, retrieved on April 26, 2011

Gonzalez, E., 2010, “*Free-to-Play Game Industry Executives Discuss Shifting Business Models at PlaySpan Monetization Forum*” on PR Web: <http://www.prweb.com/releases/2010/10/prweb4665374.htm> retrieved on May 3, 2011

Kadayifcioglu, T., 2009, *Branding in Video Games Compilation,* on Futurelab (<http://www.futurelab.net/blogs/business-games/2009/04/branding_video_games_compilati.html>), retrieved 19th of April, 2011

Latif, L., 2010, “Ubisoft’s DRM shot to pieces” on the Inquirer: <http://www.theinquirer.net/inquirer/feature/1595640/ubisoft-drm-shot-pieces>, retrieved April 18, 2011

Lowensohn, J., 2010, “*How to get DRM-free PC Games: Just Wait”,* on Cnet News: <http://news.cnet.com/8301-27076_3-20000506-248.html>, retrieved on March 27, 2011

Mattas, J., 2010 "*Blizzard: Fighting Piracy with DRM 'A Losing Battle'",* on Shacknews: http://www.shacknews.com/article/64015/blizzard-fighting-piracy-with-drm, retrieved May 3, 2011

**Meyer, de, A., Dutta S., Srivastava, S** (2002): The Bright Stuff, Financial Times/Prentice Hall

Orland, K., 2011,*”Turbine: Lord of the Rings online Revenue Tripled as Free-to-Play Game”* on Gamasutra: <http://www.gamasutra.com/view/news/32322/Turbine_Lord_of_the_Rings_Online_Revenues_Tripled_As_FreeToPlay_Game.php>, retrieved on April 28, 2011

Peuter, de, G., Dyer-Witheford, ND., Kline, S., 2003: Digital Play: The Interaction of Technology, Culture, and Marketing, McGill-Queen’s University Press

Porter, W., 2010, “DRM: Necessary Evil or Consumer Insult?” on Games Radar: <http://www.gamesradar.com/f/drm-necessary-evil-or-consumer-insult/a-20100518133549635045> retrieved April 20, 2011

Rosen, D.,2008 *“Another view of Video Game Piracy”,* <http://www.kotaku.com.au/2010/05/another-view-of-video-game-piracy/> retrieved April 26, 2011

Scott, D.M., 2008, *“The New Rules of Viral Marketing: How Word-of-Mouse Spreads your Ideas for Free”,* taken from <http://www.davidmeermanscott.com/documents/Viral_Marketing.pdf> retrieved April 26, 2011

Simmonds, N., 2010, “*Ubisoft explains DRM controversy”* on MyGaming: <http://www.mygaming.co.za/news/news/5425-Ubisoft-explains-DRM-controversy.html> retrieved April 28, 2011

Steinberg, S., 2010, *“Video Game Piracy, is it Good for Business?* On CNN News: <http://edition.cnn.com/2010/TECH/gaming.gadgets/09/09/video.game.piracy/> retrieved April 26, 2011

The Spin Project, 2007, “*Online Communications”* on Spin Project: <http://www.spinproject.org/downloads/onlinecomms.pdf>, retrieved on May 13, 2011

Walsh, I., 2009, *“Success stories for the micro-transaction business model”* on Ivan Walsh’ personal website:

<http://www.ivanwalsh.com/technical-writing-tips-tools/success-stories-for-the-micro-transaction-business-model/2434/>, retrieved on April 28, 2011

Writer, M., n.d., *“Disadvantages of Viral Marketing”* on Hubpages: <http://hubpages.com/hub/Disadvantages-of-Viral-Marketing>, retrieved on April 26, 2011

Yee, N., 2004, *“Project Daedalus Gateway- a research into MMO’s”* on Nick Yee’s personal site: <http://www.nickyee.com/daedalus/gateway_intro.html>, retrieved on April 28, 2011

Yonzon, Y., 2008, "*Microtransactions, an Asian Perspective"* on Joystiq: http://massively.joystiq.com/2008/02/27/microtransactions-an-asian-perspective/, retrieved May 3, 2011

**Reference Materials**

**Reference Articles**

(4Chan, 2011) http://boards.4chan.org/v/ "/v/- Video Games", retrieved May 22, 2011

(Brand Marketing Website, 2010) <http://www.brandmarketing.co.uk/> “Brand Marketing”. Retrieved May 8, 2011

(CD Projekt FAQ, 2011) <http://tw2.thewitcher.com/images/newsletter/TW2_FAQ_April2011.pdf> “FAQ with the Developers of *“The Witcher 2”.* Retrieved April 28, 2011

(Computers and Games Blog, 2010) <http://www.computerandvideogames.com/235596/blog/ubi-drm-their-side-of-the-story/?site=pcg> “Interview with Ubisoft’s DRM Proponent”. Retrieved May 2, 2011

(Digital Media Copyright Directive, 1998) <http://www.copyright.gov/legislation/dmca.pdf> “The Digital Media Copyright Directive”. Retrieved April 2, 2011

(DRM News, 2010) <http://www.thedrmnews.com/tag/ubisoft/> “DRM News; Tagged Ubisoft”. Retrieved April 28, 2011

(Electronic Arts, 2011) <http://aboutus.ea.com/companylabels.action> “The Official Electronic Arts Website”, retrieved April 19, 2011

(Electronic Frontier Foundation, 2009) <https://www.eff.org/> “The Electronic Frontier Foundation, Anti-DRM”. Retrieved April 2, 2011

(Escapist Magazine, 2011) <http://www.escapistmagazine.com/news/view/107233-iPhone-Game-Dev-Credits-Piracy-for-Doubling-His-Sales> “Independent Game Developer Credits Piracy for Doubling his Sales”. Retrieved April 28, 2011

(Gamdo and TorrentFreak, 2010), <http://gamdo.co.uk/> in combination with [www.torrentfreak.com](http://www.torrentfreak.com) – “PC Game Downloads in 2010”. Retrieved May 13, 2011

(Game by Night, 2010 )<http://www.gamebynight.com/?p=2095> Retrieved April 28, 2011

(Gamerfeed, 2010) <http://gamrfeed.vgchartz.com/story/82430/steam-reaches-30-million-accounts/> “Steam Reaches 30 Million Accounts”. Retrieved April 15, 2011

(Government Accountability Office, 2010)<http://www.gao.gov/new.items/d10423.pdf> “Exaggeration of Piracy Figures”. Retrieved April 18, 2011

(Ijji Forums, 2011), <http://forums.ijji.com/forumdisplay.php?f=28> “Complaints on Game Balance”. Retrieved April 29, 2011

(Keen and Graev, 2010) <http://www.keenandgraev.com/?p=4257>, retrieved April 28, 2011

(Lord of the Rings Online Forum, 2011) <http://forums.lotro.com/showthread.php?335121-Ohoh...-LOTRO-free-to-play> Retrieved April 28, 2011

(Marketing Power, 2011) [www.marketingpower.com](http://www.marketingpower.com) “The American Marketing Association”. Retrieved April 10, 2011

(Pirate Bay Forums, 2011)<http://forum.suprbay.org/polls.php?action=showresults&pid=759> “Open Poll for Pirate Bay Users”. Retrieved May 20, 2011

(Research Communications Lab, 2006) <http://www.researchcommunications.com/html/rcl_branding_model.html> “RCL Branding Model”. Retrieved May 10, 2011

(Securom, 2010) <http://www2.securom.com/SonyDADC-SecuROM.1.0.html> “Securom- The Secure DRM Solution”. Retrieved April 2, 2011

(Small Business Marketing, 2010) <http://www.smallbusinesssem.com/9-great-marketing-quotes/3426/> “Marketing Business Quotes”. Retrieved April 2, 2011

(Steam Forums, n.d.), <http://forums.steampowered.com/forums/showthread.php?t=1544139> – “User Complaints about the Team Fortress 2 Cash Shop” on Valve’s Steam Forums. Retrieved April 29, 2011

(Team Fortress 2 Website, 2010 ),<http://www.teamfortress.com/mannconomy/FAQ/> - “Valve’s FAQ About the TF2 Item Store”. Retrieved April 29, 2011

(Techdirt, 2011)<http://www.techdirt.com/articles/20110216/23141213139/maybe-super-cheap-video-games-are-helping-not-destroying-video-game-industry.shtml> - “Maybe Super Cheap Video Games are Helping, not Destroying the Video Game Industry”. Retrieved April 19, 2011

(Wired, 2009)<http://www.wired.com/gamelife/2009/03/ea-drops-invasi/> “EA Drops invasive DRM for Sims 3”, 2009, on Wired. Retrieved April 19, 2011

(Wolfire Blog, 2010 )<http://blog.wolfire.com/2010/03/DRM-can-be-effective> “DRM can be Effective”. Retrieved April 18, 2011

(XKCD) xkcd.com "Steal this Comic", retrieved June 1, 2011

(Your Brand is Showing, 2010) <http://yourbrandisshowing.tumblr.com/post/781038168/emotions-in-video-game-communications> “Emotions in Video Game Communication”. Retrieved May 8, 2011

(Youtube, 2009) <http://www.youtube.com/watch?v=pLC_zZ5fqFk> “Gabe Newell on Piracy and the Future of the Gaming Industry”. Retrieved May 2, 2011

(Youtube, 2010) http://www.youtube.com/watch?v=n7Te5fcnrUA "Official Gears of War 3 Trailer", Retrieved May 2, 2011

**List of Footnotes**

Just Cause Avalanche Studio’s talks about PC gaming, video game piracy and DRM http://gamrconnect.vgchartz.com/thread.php?id=126420 -Page 6

2http://blog.wolfire.com/2010/03/DRM-can-be-effective on effective DRM -Page 6

3DRM: A necessary evil or a consumer insult? http://www.gamesradar.com/f/drm-necessary-evil-or-consumer-insult/a-20100518133549635045 -Page 6

4 "Gabe Newell on Piracy and the future of the Gaming Industry": http://www.youtube.com/watch?v=pLC\_zZ5fqFk -Page 12

5 "Blizzard: Fighting Piracy with DRM 'A Losing Battle'": http://www.shacknews.com/article/64015/blizzard-fighting-piracy-with-drm -Page 12

6 "Ubi DRM: Their side of the Story": http://www.computerandvideogames.com/235596/blog/ubi-drm-their-side-of-the-story/?site=pcg - Page 12

7 Shelf-life being the average time it takes for a video game to “fade out” of popularity, marked by a decrease in sales. Extending shelf-life is often done via Downloadable Content or expansion packs. - Page 13

8“*Interview with Gabe Newell Regarding Piracy and the Future of Gaming”:*

http://www.youtube.com/watch?v=pLC\_zZ5fqFk -Page 20

9 “*Ubi DRM: Their side of the Story”* http://www.computerandvideogames.com/235596/blog/ubi-drm-their-side-of-the-story/?site=pcg - Page 20

10 *“Online Poll Regarding Piracy and DRM”* http://forum.suprbay.org/showthread.php?tid=89051 -Page 20

11 “*Online Communications”* http://www.spinproject.org/downloads/onlinecomms.pdf - Page 21

12"*Official Gears of War 3 Trailer*" http://www.youtube.com/watch?v=n7Te5fcnrUA- Page 26

13 "*CDProjekt RED newsletter: Removal of DRM on The Witcher2:* http://tw2.thewitcher.com/images/newsletter/TW2\_FAQ\_April2011.pdf - Page 32

14*"What are your thoughts on DRM?":* http://forum.suprbay.org/showthread.php?tid=89051 – A poll on the feeling on DRM, taken from the Pirate Bay - Page 35

15 *“An Interview with Matt Milahy, CEO of Iron Realms Entertainment”* http://www.playnoevil.com/serendipity/index.php?/archives/765-The-World-of-text-MMOs-MUDs-An-Interview-with-Matt-Mihaly,-CEO-of-Iron-Realms-Entertainment.html - Page 41

16 *“Lord of the Rings online profit tripled since free-to-play introduction”:* http://www.gamasutra.com/view/news/32322/Turbine\_Lord\_of\_the\_Rings\_Online\_Revenues\_Tripled\_As\_FreeToPlay\_Game.php - Page 42

17 Free-to-Play refers to games which are essentially free, but offering additional content via micropayments. - Page 54

18 Games which are essentially copies of other, often better-selling games, hoping to achieve sales via copying the premise- Page 54

19 Micro transactions work best on an initially free product- Page 56

**Appendix A: The Digital Millennium Copyright Act**

**THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998**

**U.S. Copyright Office Summary**



**December 1998**

**INTRODUCTION**

The Digital Millennium Copyright Act (DMCA)1

was signed into law by

President Clinton on October 28, 1998. The legislation implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The DMCA also addresses a number of other significant copyright-related issues.

The DMCA is divided into five titles:

 Title I, the “**WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998**,” implements the WIPO treaties.

 Title II, the “**Online Copyright Infringement Liability Limitation Act**,” creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.

 Title III, the “**Computer Maintenance Competition Assurance Act**,” creates an exemption for making a copy of a computer program by activating a computer for purposes of maintenance or repair.

 Title IV contains six **miscellaneous provisions**, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, “webcasting” of sound recordings on the Internet, and the applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.

 Title V, the “**Vessel Hull Design Protection Act**,” creates a new form of protection for the design of vessel hulls.

This memorandum summarizes briefly each title of the DMCA. It provides merely an overview of the law’s provisions; for purposes of length and readability a significant amount of detail has been omitted. **A complete understanding of any provision of the DMCA requires reference to the text of the legislation itself.**

1Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

*Copyright Office Summary December 1998 Page 1*

*The Digital Millennium Copyright Act of 1998*

**TITLE I: WIPO TREATY IMPLEMENTATION**

Title I implements the WIPO treaties. First, it makes certain technical amendments to U.S. law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions. In addition, Title I requires the U.S. Copyright Office to perform two joint studies with the National Telecommunications and Information Administration of the Department of Commerce (NTIA).

**Technical Amendments**

***National Eligibility***

The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) each require member countries to provide protection to certain works from other member countries or created by nationals of other member countries. That protection must be no less favorable than that accorded to domestic works.

Section 104 of the Copyright Act establishes the conditions of eligibility for protection under U.S. law for works from other countries. Section 102(b) of the DMCA amends section 104 of the Copyright Act and adds new definitions to section

101 of the Copyright Act in order to extend the protection of U.S. law to those works required to be protected under the WCT and the WPPT.

***Restoration of Copyright Protection***

Both treaties require parties to protect preexisting works from other member countries that have not fallen into the public domain in the country of origin through the expiry of the term of protection. A similar obligation is contained in both the Berne Convention and the TRIPS Agreement. In 1995 this obligation was imple- mented in the Uruguay Round Agreements Act, creating a new section 104A in the Copyright Act to restore protection to works from Berne or WTO member countries that are still protected in the country of origin, but fell into the public domain in the United States in the past because of a failure to comply with formalities that then existed in U.S. law, or due to a lack of treaty relations. Section 102(c) of the DMCA amends section 104A to restore copyright protection in the same circumstances to works from WCT and WPPT member countries.

*Copyright Office Summary December 1998 Page 2*

*The Digital Millennium Copyright Act of 1998*

***Registration as a Prerequisite to Suit***

The remaining technical amendment relates to the prohibition in both treaties against conditioning the exercise or enjoyment of rights on the fulfillment of formalities. Section 411(a) of the Copyright Act requires claims to copyright to be registered with the Copyright Office before a lawsuit can be initiated by the copyright owner, but exempts many foreign works in order to comply with existing treaty obligations under the Berne Convention. Section 102(d) of the DMCA amends section

411(a) by broadening the exemption to cover all foreign works.

**Technological Protection and Copyright Management Systems**

Each of the WIPO treaties contains virtually identical language obligating member states to prevent circumvention of technological measures used to protect copyrighted works, and to prevent tampering with the integrity of copyright management information. These obligations serve as technological adjuncts to the exclusive rights granted by copyright law. They provide legal protection that the international copyright community deemed critical to the safe and efficient exploitation of works on digital networks.

***Circumvention of Technological Protection Measures***

**General approach**

Article 11 of the WCT states:

Contracting Parties shall provide adequate legal protec- tion and effective legal remedies against the circumven- tion of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Article 18 of the WPPT contains nearly identical language.

Section 103 of the DMCA adds a new chapter 12 to Title 17 of the U.S. Code. New section 1201 implements the obligation to provide adequate and effective protection against circumvention of technological measures used by copyright owners to protect their works.

Section 1201 divides technological measures into two categories: measures that prevent unauthorized *access* to a copyrighted work and measures that prevent

*Copyright Office Summary December 1998 Page 3*

*The Digital Millennium Copyright Act of 1998*

unauthorized *copying*2 of a copyrighted work. Making or selling devices or services that are used to circumvent either category of technological measure is prohibited in certain circumstances, described below. As to the act of circumvention in itself, the provision prohibits circumventing the first category of technological measures, but not the second.

This distinction was employed to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumvent- ing a technological measure that prevents copying. By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited.

Section 1201 proscribes devices or services that fall within any one of the following three categories:

 they are primarily designed or produced to circumvent;

 they have only limited commercially significant purpose or use other

than to circumvent; or

 they are marketed for use in circumventing.

**No mandate**

Section 1201 contains language clarifying that the prohibition on circumvention devices does not require manufacturers of consumer electronics, telecommunications or computing equipment to design their products affirmatively to respond to any particular technological measure. (Section 1201(c)(3)). Despite this general ‘no mandate’ rule, section 1201(k) does mandate an affirmative response for one particular type of technology: within 18 months of enactment, all analog videocassette recorders must be designed to conform to certain defined technologies, commonly known as Macrovision, currently in use for preventing unauthorized copying of analog videocassettes and certain analog signals. The provision prohibits rightholders from applying these specified technologies to free television and basic and extended basic tier cable broadcasts.

2“Copying” is used in this context as a short-hand for the exercise of any of the exclus- ive rights of an author under section 106 of the Copyright Act. Consequently, a technological measure that prevents unauthorized distribution or public performance of a work would fall in this second category.

*Copyright Office Summary December 1998 Page 4*

*The Digital Millennium Copyright Act of 1998*

**Savings clauses**

Section 1201 contains two general savings clauses. First, section 1201(c)(1) states that nothing in section 1201 affects rights, remedies, limitations or defenses to copyright infringement, including fair use. Second, section 1201(c)(2) states that nothing in section 1201 enlarges or diminishes vicarious or contributory copyright infringement.

**Exceptions**

Finally, the prohibitions contained in section 1201 are subject to a number of exceptions. One is an exception to the operation of the entire section, for law enforcement, intelligence and other governmental activities. (Section 1201(e)). The others relate to section 1201(a), the provision dealing with the category of technological measures that control access to works.

The broadest of these exceptions, section 1201(a)(1)(B)-(E), establishes an ongoing administrative rule-making proceeding to evaluate the impact of the prohibition against the act of circumventing such access-control measures. This conduct prohibition does not take effect for two years. Once it does, it is subject to an exception for users of a work which is in a particular class of works if they are or are likely to be adversely affected by virtue of the prohibition in making noninfringing uses. The applicability of the exemption is determined through a periodic rulemaking by the Librarian of Congress, on the recommendation of the Register of Copyrights, who is to consult with the Assistant Secretary of Commerce for Communications and Information.

The six additional exceptions are as follows:

1. ***Nonprofit library, archive and educational institution exception*** (section 1201(d)). The prohibition on the act of circumvention of access control measures is subject to an exception that permits nonprofit libraries, archives and educational institutions to circumvent solely for the purpose of making a good faith determination as to whether they wish to obtain authorized access to the work.

2. ***Reverse engineering*** (section 1201(f)). This exception permits circumvention, and the development of technological means for such circumvention, by a person who has lawfully obtained a right to use a copy of a computer program for the sole purpose of identifying and analyzing elements of the program necessary to achieve interoperability with other programs, to the extent that such acts are permitted under copyright law.

3. ***Encryption research*** (section 1201(g)). An exception for encryption research permits circumvention of access control measures, and the

*Copyright Office Summary December 1998 Page 5*

*The Digital Millennium Copyright Act of 1998*

development of the technological means to do so, in order to identify flaws and vulnerabilities of encryption technologies.

4. ***Protection of minors*** (section 1201(h)). This exception allows a court applying the prohibition to a component or part to consider the necessity for its incorporation in technology that prevents access of minors to material on the Internet.

5. ***Personal privacy*** (section 1201(i)). This exception permits circumven- tion when the technological measure, or the work it protects, is capable of collecting or disseminating personally identifying information about the online activities of a natural person.

6. ***Security testing*** (section 1201(j)). This exception permits circumven- tion of access control measures, and the development of technological means for such circumvention, for the purpose of testing the security of a computer, computer system or computer network, with the authorization of its owner or operator.

Each of the exceptions has its own set of conditions on its applicability, which are beyond the scope of this summary.

***Integrity of Copyright Management Information***

Article 12 of the WCT provides in relevant part:

Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringe- ment of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broad- cast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

Article 19 of the WPPT contains nearly identical language.

New section 1202 is the provision implementing this obligation to protect the integrity of copyright management information (CMI). The scope of the protection

*Copyright Office Summary December 1998 Page 6*

*The Digital Millennium Copyright Act of 1998*

is set out in two separate paragraphs, the first dealing with false CMI and the second with removal or alteration of CMI. Subsection (a) prohibits the knowing provision or distribution of false CMI, if done with the intent to induce, enable, facilitate or conceal infringement. Subsection (b) bars the intentional removal or alteration of CMI without authority, as well as the dissemination of CMI or copies of works, knowing that the CMI has been removed or altered without authority. Liability under subsection (b) requires that the act be done with knowledge or, with respect to civil remedies, with reasonable grounds to know that it will induce, enable, facilitate or conceal an infringement.

Subsection (c) defines CMI 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, and such other information as the Register of Copyrights may prescribe by regulation. Information concerning users of works is explicitly excluded.

Section 1202 is subject to a general exemption for law enforcement, intelligence and other governmental activities. (Section 1202(d)). It also contains limitations on the liability of broadcast stations and cable systems for removal or alteration of CMI in certain circumstances where there is no intent to induce, enable, facilitate or conceal an infringement. (Section 1202(e)).

***Remedies***

Any person injured by a violation of section 1201 or 1202 may bring a civil action in Federal court. Section 1203 gives courts the power to grant a range of equitable and monetary remedies similar to those available under the Copyright Act, including statutory damages. The court has discretion to reduce or remit damages in cases of innocent violations, where the violator proves that it was not aware and had no reason to believe its acts constituted a violation. (Section 1203(c)(5)(A)). Special protection is given to nonprofit libraries, archives and educational institutions, which are entitled to a complete remission of damages in these circumstances. (Section

1203(c)(5)(B)).

In addition, it is a criminal offense to violate section 1201 or 1202 wilfully and for purposes of commercial advantage or private financial gain. Under section 1204 penalties range up to a $500,000 fine or up to five years imprisonment for a first offense, and up to a $1,000,000 fine or up to 10 years imprisonment for subsequent offenses. Nonprofit libraries, archives and educational institutions are entirely exempted from criminal liability. (Section 1204(b)).

*Copyright Office Summary December 1998 Page 7*

*The Digital Millennium Copyright Act of 1998*

**Copyright Office and NTIA Studies Relating to Technological Develop- ment**

Title I of the DMCA requires the Copyright Office to conduct two studies jointly with NTIA, one dealing with encryption and the other with the effect of technological developments on two existing exceptions in the Copyright Act. New section 1201(g)(5) of Title 17 of the U.S. Code requires the Register of Copyrights and the Assistant Secretary of Commerce for Communications and Information to report to the Congress no later than one year from enactment on the effect that the exemption for encryption research (new section 1201(g)) has had on encryption research, the development of encryption technology, the adequacy and effectiveness of technological measures designed to protect copyrighted works, and the protection of copyright owners against unauthorized access to their encrypted copyrighted works.

Section 104 of the DMCA requires the Register of Copyrights and the Assistant Secretary of Commerce for Communications and Information to jointly evaluate (1) the effects of Title I of the DMCA and the development of electronic commerce and associated technology on the operation of sections 109 (first sale doctrine) and 117 (exemption allowing owners of copies of computer programs to reproduce and adapt them for use on a computer), and (2) the relationship between existing and emergent technology and the operation of those sections. This study is due 24 months after the date of enactment of the DMCA.

**TITLE II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

Title II of the DMCA adds a new section 512 to the Copyright Act3 to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

1. Transitory communications;

2. System caching;

3. Storage of information on systems or networks at direction of users;

and

4. Information location tools.

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

3The Fairness in Musical Licensing Act, Title II of Pub. L. No. 105-298, 112 Stat. 2827,

2830-34 (Oct. 27, 1998) also adds a new section 512 to the Copyright Act. This duplication of section numbers will need to be corrected in a technical amendments bill.

*Copyright Office Summary December 1998 Page 8*

*The Digital Millennium Copyright Act of 1998*

Each limitation entails a complete bar on monetary damages, and restricts the availability of injunctive relief in various respects. (Section 512(j)). Each limitation relates to a separate and distinct function, and a determination of whether a service provider qualifies for one of the limitations does not bear upon a determination of whether the provider qualifies for any of the other three. (Section 512(n)).

The failure of a service provider to qualify for any of the limitations in section

512 does not necessarily make it liable for copyright infringement. The copyright

owner must still demonstrate that the provider has infringed, and the provider may still

avail itself of any of the defenses, such as fair use, that are available to copyright

defendants generally. (Section 512(l)).

In addition to limiting the liability of service providers, Title II establishes a procedure by which a copyright owner can obtain a subpoena from a federal court ordering a service provider to disclose the identity of a subscriber who is allegedly engaging in infringing activities. (Section 512(h)).

Section 512 also contains a provision to ensure that service providers are not placed in the position of choosing between limitations on liability on the one hand and preserving the privacy of their subscribers, on the other. Subsection (m) explicitly states that nothing in section 512 requires a service provider to monitor its service or access material in violation of law (such as the Electronic Communications Privacy Act) in order to be eligible for any of the liability limitations.

**Eligibility for Limitations Generally**

A party seeking the benefit of the limitations on liability in Title II must qualify as a “service provider.” For purposes of the first limitation, relating to transitory communications, “service provider” is defined in section 512(k)(1)(A) as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” For purposes of the other three limitations, “service provider” is more broadly defined in section 512(k)(l)(B) as “a provider of online services or network access, or the operator of facilities therefor.”

In addition, to be eligible for any of the limitations, a service provider must meet two overall conditions: (1) it must adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; and (2) it must accommodate and not interfere with “standard technical measures.” (Section 512(i)). “Standard technical measures” are defined as measures that copyright owners use to identify or protect copyrighted works, that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, are available to anyone on

*Copyright Office Summary December 1998 Page 9*

*The Digital Millennium Copyright Act of 1998*

reasonable nondiscriminatory terms, and do not impose substantial costs or burdens on service providers.

**Limitation for Transitory Communications**

In general terms, section 512(a) limits the liability of service providers in circumstances where the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else’s request. This limitation covers acts of transmission, routing, or providing connections for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network.

In order to qualify for this limitation, the service provider’s activities must meet the following conditions:

 The transmission must be initiated by a person other than the provider.

 The transmission, routing, provision of connections, or copying must

be carried out by an automatic technical process without selection of

material by the service provider.

 The service provider must not determine the recipients of the material.

 Any intermediate copies must not ordinarily be accessible to anyone

other than anticipated recipients, and must not be retained for longer

than reasonably necessary.

 The material must be transmitted with no modification to its content.

**Limitation for System Caching**

Section 512(b) limits the liability of service providers for the practice of retaining copies, for a limited time, of material that has been made available online by a person other than the provider, and then transmitted to a subscriber at his or her direction. The service provider retains the material so that subsequent requests for the same material can be fulfilled by transmitting the retained copy, rather than retrieving the material from the original source on the network.

The benefit of this practice is that it reduces the service provider’s bandwidth requirements and reduces the waiting time on subsequent requests for the same information. On the other hand, it can result in the delivery of outdated information to subscribers and can deprive website operators of accurate “hit” information — information about the number of requests for particular material on a website — from which advertising revenue is frequently calculated. For this reason, the person making the material available online may establish rules about updating it, and may utilize technological means to track the number of “hits.”

*Copyright Office Summary December 1998 Page 10*

*The Digital Millennium Copyright Act of 1998*

The limitation applies to acts of intermediate and temporary storage, when carried out through an automatic technical process for the purpose of making the material available to subscribers who subsequently request it. It is subject to the following conditions:

 The content of the retained material must not be modified.

 The provider must comply with rules about “refreshing” mate-

rial—replacing retained copies of material with material from the

original location— when specified in accordance with a generally

accepted industry standard data communication protocol.

 The provider must not interfere with technology that returns “hit”

information to the person who posted the material, where such

technology meets certain requirements.

 The provider must limit users’ access to the material in accordance with

conditions on access (e.g., password protection) imposed by the person

who posted the material.

 Any material that was posted without the copyright owner’s authoriza-

tion must be removed or blocked promptly once the service provider

has been notified that it has been removed, blocked, or ordered to be

removed or blocked, at the originating site.

**Limitation for Information Residing on Systems or Networks at the**

**Direction of Users**

Section 512(c) limits the liability of service providers for infringing material on websites (or other information repositories) hosted on their systems. It applies to storage at the direction of a user. In order to be eligible for the limitation, the following conditions must be met:

 The provider must not have the requisite level of knowledge of the infringing activity, as described below.

 If the provider has the right and ability to control the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity.

 Upon receiving proper notification of claimed infringement, the provider must expeditiously take down or block access to the material.

In addition, a service provider must have filed with the Copyright Office a designation of an agent to receive notifications of claimed infringement. The Office provides a suggested form for the purpose of designating an agent [(http://www.loc.gov/copyright/onlinesp/)](http://www.loc.gov/copyright/onlinesp/) and maintains a list of agents on the Copyright Office website [(http://www.loc.gov/copyright/onlinesp/list/).](http://www.loc.gov/copyright/onlinesp/list/)

*Copyright Office Summary December 1998 Page 11*

*The Digital Millennium Copyright Act of 1998*

Under the knowledge standard, a service provider is eligible for the limitation on liability only if it does not have actual knowledge of the infringement, is not aware of facts or circumstances from which infringing activity is apparent, or upon gaining such knowledge or awareness, responds expeditiously to take the material down or block access to it.

The statute also establishes procedures for proper notification, and rules as to its effect. (Section 512(c)(3)). Under the notice and takedown procedure, a copyright owner submits a notification under penalty of perjury, including a list of specified elements, to the service provider’s designated agent. Failure to comply substantially with the statutory requirements means that the notification will not be considered in determining the requisite level of knowledge by the service provider. If, upon receiving a proper notification, the service provider promptly removes or blocks access to the material identified in the notification, the provider is exempt from monetary liability. In addition, the provider is protected from any liability to any person for claims based on its having taken down the material. (Section 512(g)(1)).

In order to protect against the possibility of erroneous or fraudulent notifications, certain safeguards are built into section 512. Subsection (g)(1) gives the subscriber the opportunity to respond to the notice and takedown by filing a counter notification. In order to qualify for the protection against liability for taking down material, the service provider must promptly notify the subscriber that it has removed or disabled access to the material. If the subscriber serves a counter notification complying with statutory requirements, including a statement under penalty of perjury that the material was removed or disabled through mistake or misidentification, then unless the copyright owner files an action seeking a court order against the subscriber, the service provider must put the material back up within 10-14 business days after receiving the counter notification.

Penalties are provided for knowing material misrepresentations in either a notice or a counter notice. Any person who knowingly materially misrepresents that material is infringing, or that it was removed or blocked through mistake or misidentifi- cation, is liable for any resulting damages (including costs and attorneys’ fees) incurred by the alleged infringer, the copyright owner or its licensee, or the service provider. (Section 512(f)).

**Limitation for Information Location Tools**

Section 512(d) relates to hyperlinks, online directories, search engines and the like. It limits liability for the acts of referring or linking users to a site that contains infringing material by using such information location tools, if the following conditions are met:

*Copyright Office Summary December 1998 Page 12*

*The Digital Millennium Copyright Act of 1998*

 The provider must not have the requisite level of knowledge that the material is infringing. The knowledge standard is the same as under the limitation for information residing on systems or networks.

 If the provider has the right and ability to control the infringing activity, the provider must not receive a financial benefit directly attributable to the activity.

 Upon receiving a notification of claimed infringement, the provider must expeditiously take down or block access to the material.

These are essentially the same conditions that apply under the previous limitation, with some differences in the notification requirements. The provisions establishing safeguards against the possibility of erroneous or fraudulent notifications, as discussed above, as well as those protecting the provider against claims based on having taken down the material apply to this limitation. (Sections 512(f)-(g)).

**Special Rules Regarding Liability of Nonprofit Educational Institutions**

Section 512(e) determines when the actions or knowledge of a faculty member or graduate student employee who is performing a teaching or research function may affect the eligibility of a nonprofit educational institution for one of the four limitations on liability. As to the limitations for transitory communications or system caching, the faculty member or student shall be considered a “person other than the provider,” so as to avoid disqualifying the institution from eligibility. As to the other limitations, the knowledge or awareness of the faculty member or student will not be attributed to the institution. The following conditions must be met:

 the faculty member or graduate student’s infringing activities do not involve providing online access to course materials that were required or recommended during the past three years;

 the institution has not received more than two notifications over the past three years that the faculty member or graduate student was infringing; and

 the institution provides all of its users with informational materials describing and promoting compliance with copyright law.

**TITLE III: COMPUTER MAINTENANCE OR REPAIR**

Title III expands the existing exemption relating to computer programs in section 117 of the Copyright Act, which allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer. The exemption only permits a copy that is made automatically when a computer is activated, and only if the computer already lawfully

*Copyright Office Summary December 1998 Page 13*

*The Digital Millennium Copyright Act of 1998*

contains an authorized copy of the program. The new copy cannot be used in any other manner and must be destroyed immediately after the maintenance or repair is completed.

**TITLE IV: MISCELLANEOUS PROVISIONS**

**Clarification of the Authority of the Copyright Office**

Section 401(b), adds language to section 701 of the Copyright Act confirming the Copyright Office’s authority to continue to perform the policy and international functions that it has carried out for decades under its existing general authority.

**Ephemeral Recordings for Broadcasters**

Section 112 of the Copyright Act grants an exemption for the making of “ephemeral recordings.” These are recordings made in order to facilitate a transmis- sion. Under this exemption, for example, a radio station can record a set of songs and broadcast from the new recording rather than from the original CDs (which would have to be changed “on the fly” during the course of a broadcast).

As it existed prior to enactment of the DMCA, section 112 permitted a transmitting organization to make and retain for up to six months (hence the term “ephemeral”) no more than one copy of a work if it was entitled to transmit a public performance or display of the work, either under a license or by virtue of the fact that there is no general public performance right in sound recordings (as distinguished from musical works).

The Digital Performance Right in Sound Recordings Act of 1995 (DPRA) created, for the first time in U.S. copyright law, a limited public performance right in sound recordings. The right only covers public performances by means of digital transmission and is subject to an exemption for digital broadcasts (i.e., transmissions by FCC licensed terrestrial broadcast stations) and a statutory license for certain subscription transmissions that are not made on demand (i.e. in response to the specific request of a recipient).

Section 402 of the DMCA expands the section 112 exemption to include recordings that are made to facilitate the digital transmission of a sound recording where the transmission is made under the DPRA’s exemption for digital broadcasts or statutory license. As amended, section 112 also permits in some circumstances the circumvention of access control technologies in order to enable an organization to make an ephemeral recording.

*Copyright Office Summary December 1998 Page 14*

*The Digital Millennium Copyright Act of 1998*

**Distance Education Study**

In the course of consideration of the DMCA, legislators expressed an interest in amending the Copyright Act to promote distance education, possibly through an expansion of the existing exception for instructional broadcasting in section 110(2). Section 403 of the DMCA directs the Copyright Office to consult with affected parties and make recommendations to Congress on how to promote distance education through digital technologies. The Office must report to Congress within six months of enactment.

The Copyright Office is directed to consider the following issues:

 The need for a new exemption;

 Categories of works to be included in any exemption;

 Appropriate quantitative limitations on the portions of works that may

be used under any exemption;

 Which parties should be eligible for any exemption;

 Which parties should be eligible recipients of distance education

material under any exemption;

 The extent to which use of technological protection measures should

be mandated as a condition of eligibility for any exemption;

 The extent to which the availability of licenses should be considered in

assessing eligibility for any exemption; and

 Other issues as appropriate.

**Exemption for Nonprofit Libraries and Archives**

Section 404 of the DMCA amends the exemption for nonprofit libraries and archives in section 108 of the Copyright Act to accommodate digital technologies and evolving preservation practices. Prior to enactment of the DMCA, section 108 permitted such libraries and archives to make a single facsimile (i.e., not digital) copy of a work for purposes of preservation or interlibrary loan. As amended, section 108 permits up to three copies, which may be digital, provided that digital copies are not made available to the public outside the library premises. In addition, the amended section permits such a library or archive to copy a work into a new format if the original format becomes obsolete—that is, the machine or device used to render the work perceptible is no longer manufactured or is no longer reasonably available in the commercial marketplace.

**Webcasting Amendments to the Digital Performance Right in Sound**

**Recordings**

As discussed above, in 1995 Congress enacted the DPRA, creating a performance right in sound recordings that is limited to digital transmissions. Under

*Copyright Office Summary December 1998 Page 15*

*The Digital Millennium Copyright Act of 1998*

that legislation, three categories of digital transmissions were addressed: broadcast transmissions, which were exempted from the performance right; subscription transmissions, which were generally subject to a statutory license; and on-demand transmissions, which were subject to the full exclusive right. Broadcast transmissions under the DPRA are transmissions made by FCC-licensed terrestrial broadcast stations.

In the past several years, a number of entities have begun making digital transmissions of sound recordings over the Internet using streaming audio technolo- gies. This activity does not fall squarely within any of the three categories that were addressed in the DPRA. Section 405 of the DMCA amends the DPRA, expanding the statutory license for subscription transmissions to include webcasting as a new category of “eligible nonsubscription transmissions.”

In addition to expanding the scope of the statutory license, the DMCA revises the criteria that any entity must meet in order to be eligible for the license (other than those who are subject to a grandfather clause, leaving the existing criteria intact). It revises the considerations for setting rates as well (again, subject to a grandfather clause), directing arbitration panels convened under the law to set the royalty rates at fair market value.

This provision of the DMCA also creates a new statutory license for making ephemeral recordings. As indicated above, section 402 of the DMCA amends section

112 of the Copyright Act to permit the making of a single ephemeral recording to facilitate the digital transmission of sound recording that is permitted either under the DPRA’s broadcasting exemption or statutory license. Transmitting organizations that wish to make more than the single ephemeral recording of a sound recording that is permitted under the outright exemption in section 112 are now eligible for a statutory license to make such additional ephemeral recordings. In addition, the new statutory license applies to the making of ephemeral recordings by transmitting organizations other than broadcasters who are exempt from the digital performance right, who are not covered by the expanded exemption in section 402 of the DMCA.

**Assumption of Contractual Obligations upon Transfers of Rights in**

**Motion Pictures**

Section 416 addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments. The guilds’ collective bargaining agreements currently require producers to obtain assumption agreements from distributors in certain circumstances, by which the distributor assumes the producer’s obligation to make such residual payments. Some production companies apparently do not always do so, leaving the guilds without contractual privity enabling them to seek recourse from the distributor.

*Copyright Office Summary December 1998 Page 16*

*The Digital Millennium Copyright Act of 1998*

The DMCA adds a new chapter to Title 28 of the U.S. Code that imposes on transferees those obligations to make residual payments that the producer would be required to have the transferee assume under the relevant collective bargaining agreement. The obligations attach only if the distributor knew or had reason to know that the motion picture was produced subject to a collective bargaining agreement, or in the event of a court order confirming an arbitration award under the collective bargaining agreement that the producer cannot satisfy within ninety days. There are two classes of transfers that are excluded from the scope of this provision. The first is transfers limited to public performance rights, and the second is grants of security interests, along with any subsequent transfers from the security interest holder.

The provision also directs the Comptroller General, in consultation with the Register of Copyrights, to conduct a study on the conditions in the motion picture industry that gave rise to this provision, and the impact of the provision on the industry. The study is due two years from enactment.

**TITLE V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

Title V of the DMCA, entitled the Vessel Hull Design Protection Act (VHDPA), adds a new chapter 13 to Title 17 of the U.S. Code. It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, “useful articles” are limited to the hulls (including the decks) of vessels no longer than 200 feet.

A design is protected under the VHDPA as soon as a useful article embodying the design is made public or a registration for the design is published. Protection is lost if an application for registration is not made within two years after a design is first made public, but a design is not registrable if it has been made public more than one year before the date of the application for registration. Once registered, protection continues for ten years from the date protection begins.

The VHDPA is subject to a legislative sunset: the Act expires two years from enactment (October 28, 2000). The Copyright Office is directed to conduct two joint studies with the Patent and Trademark Office—the first by October 28, 1999 and the second by October 28, 2000—evaluating the impact of the VHDPA.

**EFFECTIVE DATES**

Most provisions of the DMCA are effective on the date of enactment. There are, however, several exceptions. The technical amendments in Title I that relate to eligibility of works for protection under U.S. copyright law by virtue of the new WIPO treaties do not take effect until the relevant treaty comes into force. Similarly, restoration of copyright protection for such works does not become effective until the relevant treaty comes into force. The prohibition on the act of circumvention of access

*Copyright Office Summary December 1998 Page 17*

*The Digital Millennium Copyright Act of 1998*

control measures does not take effect until two years from enactment (October 28,

2000).



*Copyright Office Summary December 1998 Page 18*

**Appendix B: If Piracy is the Problem, Is DRM the Answer?**



**If Piracy is the Problem, Is DRM the Answer?**

Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan

Trusted Systems Laboratory

HP Laboratories Cambridge

HPL-2003-110

May 27th , 2003\*

security, content protection, digital rights management, trust, privacy, piracy

Piracy of digital content is considered a serious problem by content companies. Digital Rights Management is considered a potential solution to this problem. In this paper we study to what degree DRM can live up to this expectation. We conclude that given the current and foreseeable state of technology the content protection features of DRM are not effective at combating piracy. The key problem is that even if only a small fraction of users are able to get content from a protected form into an unprotected form, then illegitimate distribution networks are likely to make that content available ubiquitously. One possible technological solution to the problem is what we call “draconian DRM,” which invo lves deploying devices that only process managed content. However, we find that such systems face significant, if not insurmountable, obstacles to deployment and we believe that the real solution to the piracy problem is largely non-technical. The most effective way for interested parties to defeat piracy may be to compete with it.

\* Internal Accession Date Only Approved for External Publication

To be published as a chapter in Digital Rights Management: Technological, Economic, Legal and Political Aspects, ed. Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump, Springer-Verlag, 2003

Copyright Springer-Verlag

**If Piracy is the Problem, Is DRM the Answer?**

**Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan**

Hewlett-Packard Company

**1 Summary**

Piracy of digital content is considered a serious problem by content companies. Digital Rights Management is considered a potential solution to this problem. In this paper we study to what degree DRM can live up to this expectation. We conclude that given the current and foreseeable state of technology the content protection features of DRM are not effective at combating piracy.

The key problem is that if even a small fraction of users are able to transform content from a protected to an unprotected form, then illegitimate distribution networks are likely to make that content available ubiquitously.

One possible technological solution to the problem is what we call “draconian DRM”, which involves deploying devices that only process managed content. However, we find that such systems face significant, if not insurmountable, obstacles to deployment and we believe that the real solution to the piracy problem is largely non-technical. The most effective way for interested parties to defeat piracy may be to compete with it.

Our paper is closely related to the recent paper by Biddle, et al., “The Darknet and the Future of Content Protection” [2]. Instead of focusing on the distribution network, however, we describe in more depth how DRM systems attempt to deal with various aspects of piracy, and how they fail.

**2 Piracy**

Piracy is the unauthorized use or reproduction of music, movies, books, and other types of content that are granted protection under copyright law. This kind of protection typically gives the owner of the content the exclusive right to perform certain actions on the content or to authorize others to do so. We recognize that determining whether an action is authorized or unauthorized may require protracted and subtle debate and that reasonable people may differ in their assessment of a given situation. For the purposes of this paper, however, we do not further address these subtleties for no matter how broadly or narrowly we construe piracy, we reach the same conclusion with regard to the effectiveness of DRM technologies in combating its effect.

1 This article will appear as a chapter in *Digital Rights Management: Technological, Economic, Legal and*

*Political Aspects*, ed. Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (Springer-Verlag,

2003). The opinions expressed in this article reflect solely the view of the authors and are not necessarily the view of HP.

- 1 -

There are many kinds of content that do not qualify for copyright protection because they do not contain any original authorship and are common public property. Even content that does qualify receives protection only for a limited time, after which that work becomes public property. We refer to these types of content, which are not granted copyright protection, as *public content*.

There are generally two ways in which piracy can occur:

*Unauthorized acquisition*. The form of piracy with which most people are familiar occurs when a consumer obtains copyrighted content illegitimately, for example by unauthorized downloading of content from a peer-to-peer file sharing service such as Napster or Gnutella, or by obtaining illegitimate CDs or DVDs from a

street vendor or friend2.

*Unauthorized use*. This form of piracy occurs when a consumer obtains a piece of copyrighted content legitimately and then attempts to use it in an unauthorized way.

A fundamental flaw in the debate around DRM is that it is often assumed that a solution to the second problem will solve the first as well. In this paper we explore how various DRM technologies attempt to address these two problems, and to what extent they might succeed.

**3 DRM Technologies**

The goal of a DRM system is to enforce licenses3 between a content provider (the licensor) and a consumer (the licensee) that define rules about authorized use of managed content. There are only a limited number of technologies that can be employed to build DRM systems to achieve this goal. These technologies can be broadly categorized as follows.

First, there must be a piece of software or hardware somewhere within the system that evaluates the license against a requested action, determines if that action conforms to the terms of the license, and either allows or blocks that action from occurring.

Second, there must be an *authentication* component to identify the licensee. The licensee could be a human user or a piece of hardware or software.

Third, we need a way to associate licenses with content. When content is associated with a license using some technological means, we say that the content is *managed.4* If content does not have a license associated with it, we say it is *unmanaged*. If users can somehow convert a managed piece of content into an unmanaged form, then they can use it in

2 In these situations it is usually the person doing the distribution that is called the “pirate”. Since the number of illegitimate distributions must equal the number of illegitimate consumptions, we focus on the consumer side of piracy.

3 Also known as *policies* or *digital rights.*

4 We could have used the term *protected* in this context, but *managed* fits more cleanly as we are making no claims as to the strength of the technological mechanism for linking content with its license.

- 2 -

unlimited ways. In particular, they can share it with other unauthorized users. We call such illegitimately transformed content *dissociated content*.

***3.1 General Vulnerabilities***

Typically the license-evaluating engine executes on a computing platform that is under the control of the licensee, as opposed to the licensor. Since the licensee can potentially be an adversary, we must rely on the security of the platform to ensure that the content is used in accordance with its associated license. To buttress the security of this platform we may employ tamper-resistant hardware or software components. However, there is no widely deployed trusted platform technology that has sufficient security guarantees, and it is widely accepted within the security community that such platforms can and will be

broken by determined adversaries5.

Without authentication, an attacker could attempt to deceive the license evaluation engine into thinking that a different, authorized user is attempting to use the content. While authentication systems are well understood, they are not infallible, and thus provide another target for circumventing the system. In general, the adversary may attempt to spoof other characteristics that the license evaluation engine uses to make its decision.

In the rest of this section, we discuss how various DRM technologies attempt to bind licenses to content, how those bindings can be broken, and how these technologies attempt to deal with the problem of unauthorized acquisition. The binding can be achieved externally, by cryptographic means, using what may be called “secure container methods”; or internally, as part of the content itself, either by employing watermarking methods as discussed in Section 3.3, or by using an intrinsic property of each piece of content, as with the “fuzzy hashing” technique discussed below.

***3.2 Secure Container Methods***

Many DRM systems work by distributing and storing content in an encrypted form and protecting it indirectly by managing the keys used to decrypt the content [10]. The license can be associated with the protected content in a variety of ways, for example as a header to the encrypted file. There is typically some attempt to “hide” the decryption keys from the user with tamper-resistant software or hardware methods. We call DRM systems based on this kind of technique *secure container methods*.

5 Recently much debate has arisen about the role of trusted computing platforms with regard to DRM. Much of this discussion has focused on systems such as those exemplified by the Trusted Computing Group [6] or Microsoft’s Palladium architecture, now known as *Next-Generation Secure Computing Base for Windows* (NGSCB) [5]. While these technologies can be used to strengthen the delivery of ordinary DRM capabilities, we do not believe that they are effective in combating piracy. As is argued in section 4 below, even a small number of motivated attackers is sufficient to enable widespread dissemination of content. Both TCPA and NGSCB are designed to be robust against software attacks on the platform, but with a focus on low costs these systems are not designed to withstand motivated physical attacks on the hardware. As a result, content manipulated on these systems can be assumed to be vulnerable to the determined pirate.

- 3 -

Secure container methods have a limited ability to address the piracy problem since they have no mechanisms to prevent unauthorized acquisition. They must rely on some other method to address this aspect of piracy.

Encrypting the content solves some useful problems. In particular, it allows the system to target content towards a specific device or user and prevents eavesdropping by an unauthorized party during transmission. But ultimately, we have only deferred a solution to the primary problem of preventing unauthorized use of content to that of preventing unauthorized use of the key. Consequently, we need some mechanism to manage the key in the sense above of associating it with a license.

Clearly, the licensee must eventually obtain the key to use the content. Once the key is obtained, the security of the system relies entirely on the security of the trusted platform to maintain the binding of key to content. This binding can be broken either by finding the hidden key or by modifying the license evaluation engine to release the content in an unprotected form.

Even without compromising the security of the trusted platform, there is an almost trivial approach to convert managed content to dissociated content. Content must eventually be released in an unprotected form in order for it to be consumed. Music and movies must be converted to sound waves and photons for us to enjoy it. Content can be sampled at those points in the control flow where it is no longer directly associated with a license. This problem is commonly known as *the analog hole*, because these capture points usually occur after the content has been converted from digital to analog form. But the term “analog hole” is overly restrictive, since the problem exists even while the content is still in digital form. For practical purposes, the content is often in an unprotected form in device drivers, memory, or storage long before its digital-to-analog conversion, and so can be easily captured at these points as well. Once again, we must rely on the securit y of the trusted platform to protect the content at as many of these points as best as we can. But ultimately there are points at which the content can no longer be protected.

***3.3 Watermarking***

In watermarking a signal is embedded directly into the content; the signal is imperceptible to humans, but can be detected by machines. For the purposes of this discussion, the signal represents the license associated with the content (even though, in many cases where watermarking has been proposed, the “license” is an especially simple one or is a reference to an external license specification).

We do not address here the subject of *fingerprinting*, in which the watermark represents the identity of the licensee and is typically used for forensic purposes.

Watermarking deals with the problem of unauthorized use by detecting watermarks in content and deciding whether or not the content can be used according to the license specified by the watermark. Watermarking deals with unauthorized acquisition by assuming that watermark detectors are ubiquitously embedded into all of the critical points at which content might be used.

- 4 -

To break the binding between the license and the content involves either removing the watermark or making the watermark undetectable. This is typically accomplished by applying basic data transformations to the content; for example, for images these transformations include scaling, cropping, and compression. The very ubiquity of the watermark detectors considerably eases the task of removing a watermark from a piece of content: an attacker can use the detector as part of an algorithm to remove the watermark [7]. The goal of watermarking is to make it difficult to allow these transformations to succeed without causing unacceptable perceptual distortions in the content. In fact, watermarking schemes are usually designed so that the watermarks will survive the conversion from digital to analog form. A scheme that achieved this goal would be useful in facing certain attacks via the analog hole.

Unfortunately, we cannot provide a strong security assessment of watermarking technologies. A fundamental problem with watermarking is that we only have partial theories of human perception (and we are unlikely to find one in the near future as this is an extremely difficult artificial intelligence problem). This is a double edged sword. On the one hand, it is this lack of understanding that gives us the ability to insert watermarks into content in the first place. If we did understand perception we could in principle compress all perceptually equivalent signals to the same value, leaving no bandwidth for watermarks. On the other hand, this lack of understanding means that we can give no strong security guarantees about watermarking because, at best, we must rely on empirical evidence to say that removing a watermark necessarily results in a perceptually degraded signal.

Moreover, it is not clear that any existing watermarking techniques achieve their stated goal. Most of the techniques described in the academic literature just address specific aspects of the watermarking problem, or they have later been shown to be vulnerable to attack [8]. Proprietary algorithms from technology vendors have failed to show robustness in public challenges [3] or have not been widely enough deployed to evaluate their strength.

We believe that, given this state of affairs, we have to make the assumption that watermarking will not provide any significant security in the near future. Although a number of claims for the effectiveness of watermarking have been made so far the technical reality has turned out to be disappointing.

***3.4 Fuzzy Hashing***

A relatively new alternative to secure containers and watermarking is “fuzzy hashing,” such as the Fraunhofer’s AudioID technology that has been developed recently for audio content[1]. In principle, this kind of technique could be applied to other forms of content such as video. Instead of inserting a signal into the content, as is done with watermarking, the goal of fuzzy hashing is to recognize the content directly. Unlike cryptographic hashing, where the hashes of two different pieces of data are wildly different even if the data differ by only a single bit, fuzzy hashing attempts to compute an identical hash for two pieces of content if they are perceptually equivalent. The hash

- 5 -

value can then be used as a key to query a database for the licensing information associated with a piece of content.

There are two choices for a system architecture using fuzzy hashing. Either the hashes are stored locally with the license evaluation engine, or they are stored remotely on a centralized server. If the hashes are stored locally, the list needs to be continuously updated as new content is created. The storage requirements of such a system could be potentially massive, and the cost of the device might be significant. If the hashes are stored remotely, then it is not clear how to deal with devices that are off-line.

As with watermarking, fuzzy hashing deals with unauthorized acquisition by assuming that fuzzy hash detectors are ubiquitously embedded into all of the critical points at which content might be used.

Fuzzy hashing is also heavily dependent on our understanding of human perception. To break the binding between the license and the content requires modifying the content in some way so that the hash no longer matches the hash stored in the database. Clearly, if we had complete understanding of human perception, this kind of attack would be impossible as we would design the hash functions to account for all perceptually equivalent versions of the content.

The robustness of these technologies is unknown. Public testing is needed to determine whether the algorithms can easily be fooled. Furthermore, a number of systems issues need to be resolved for a reliable infrastructure. Lastly, this technology needs to be very precise, yielding (almost) no false positives, to ensure that personal or business users would not find themselves in the situation that legitimate (public) content is not rendered. Thus, while fuzzy hashing is an interesting technical approach, there are too many unknowns at this time to justify significant hope for a solution in the near future.

**4 Ordinary vs. Draconian DRM**

We’ve seen that there are a variety of DRM solutions to deal with the problem of unauthorized use. None of these technologies is perfect, but one might imagine that they could be made secure enough to deter all but the most determined adversaries.

Furthermore, we have seen that watermarking and fuzzy hashing are the only technologies that deal with unauthorized acquisition.6 They must be deployed ubiquitously in order to be effective. One might imagine that the various stakeholders could come to some agreement on such technology, standardize it, and deploy it so that

the vast majority of devices that deal with copyrighted content would implement those technologies.

Would these two steps be enough to stop the problem of piracy? We claim that even given the optimistic hypothesis that the above conditions held, this would have little

6 Recall the “analog hole”. Only watermarking and fuzzy hashing techniques that survive analog rendering and subsequent digital recapture can be effective. Secure container systems render their content in the clear, thereby losing subsequent control of the content.

- 6 -

effect on piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

The key is that even if each user only shares his or her content with a small set of other users, the content can spread throughout the distribution network rather efficiently. Moreover skilled adversaries can turn their attack into a widely distributed tool that others who are less technically sophisticated can use, further increasing the efficiency of illegitimate content dissemination. Either way, once content is dissociated from its license, it can become widely available to all who want it.

This is why the attempts by the media and entertainment industry to shut down illegal file trading systems like Napster and Gnutella are such an important component of the industry’s strategy to battle piracy. However, as is well articulated in the Darknet paper, there are a number of technical reasons why this strategy is unlikely to succeed [2].

One of the reasons for this failure is that DRM, as it is ordinarily conceived, requires that devices handle both managed and unmanaged content simultaneously. We call systems built according to this principle *ordinary DRM*.

The only logical alternative is what we call *draconian DRM,* in which devices that handle managed content do not handle unmanaged content at all. Specifically, technology is embedded ubiquitously at key points in the content distribution chain, most notably in rendering devices, so that content cannot be used unless it has an associated license. We assume that licenses are issued by a trusted authority and are hard to forge. This solves the unauthorized acquisition problem since dissociated content will not be played, by definition.

However there are serious problems with draconian DRM. The first major hurdle is that this solution would require a complete replacement of the existing device infrastructure with DRM enabled end devices. For the sake of argument, let us assume that such a system could be agreed upon and built.

A more fundamental problem is how such a system would handle public content. And there is also the problem of how to deal with individually generated content, such as home videos, business correspondence and other such material.

There are two solutions, each with its own set of problems.

There could be two parallel infrastructures: one that handles managed content and one that handles all other content.

We could require that all content, whether managed or not, come with a license.

The problem with the first approach is that the parallel infrastructure could, and probably would, be used to support dissociated content. Therefore, the managed infrastructure must offer some value to the consumer that the other infrastructure does not. This may actually be feasible, for example, if the managed infrastructure had better features or

- 7 -

lower cost than the other infrastructure. On the other hand it is not clear that consumers would not want and that infrastructure providers would not enable those same features for unmanaged content as well.

For the second solution, the primary problem is who would issue the licenses to public or individually created content. In one scenario, this could be a centralized institution, or small set of institutions, that are globally trusted by all users. However this raises a number of issues. What should be done with content that is confidential or private? Clearly any such proposal raises a number of fundamental privacy issues. Alternatively, any content capturing device can be certified by a manufacturer and the license for content produced by the device could be certified by the device itself. However, unless playback is limited to that single device, this only delays the problem by one step. How does the recording device reliably distinguish between copyrighted and public or individually created content?

**5 Competing with Piracy**

Ordinary DRM will not prevent piracy and it is questionable whether or not draconian DRM can be effective either. Legal attacks will probably never make the Darknet completely go away. One might be tempted to toss up one’s hands and give up.

But perhaps we should not be so hasty. It is entirely feasible that DRM could at least partially affect piracy. The software industry is currently experiencing a 40% software piracy rate. Nevertheless, the software industry by all accounts appears to be thriving. Media and entertainment companies may face a similar challenge. If piracy could be decreased by just a few percentage points using DRM, then this might translate into millions of dollars of otherwise unrealized revenue.

But DRM does not come without a price. First there is the cost of building, deploying and maintaining a DRM infrastructure, which will eat into whatever unrealized revenues are recovered. Second, as pointed out in [2], DRM protected content is economically less valuable than unprotected content. So deploying DRM will result in fewer sales of legitimate content, which also might offset some of the revenues gained by decreasing piracy. The question is whether or not the benefits of DRM outweigh its costs.

Regardless of whether or not DRM can be effectively used as a risk management component, we believe that content producers must regard themselves as being in competition with the pirates. As expressed by Shapiro and Varian, “The important thing is to *maximize the value* of your intellectual property, not to protect it for the sake of protection” [9].

A historical perspective on adjusting to new technologies is useful. Many content producers reacted with alarm at the emergence of home video recording capabilities, but today video distribution is a significant vehicle for the content distribution industry. This is not an isolated case, in fact, the growth of circulating libraries and of book publishing

- 8 -

in England and the United States in the 18th and 19th centuries is analogous to the case of the video industry [11].

The assertion that content producers might do better by structuring their offerings as subscriptions (or a variation on that model) than according to a pay-per-view model has some backing from an economic analysis by Fishburn, Odlyzko, and Siders [4]. Modeling the situation of competing producers of mass-market information goods, and surveying the history of consumer preferences in several industries, they found that producers could achieve higher revenues through bundling, and that consumers' strong preference for flat rates could stimulate usage.

There are several different ways in which the content and IT industries might extend their offerings to compete with piracy.

Content management:

o *Recommendation*: A music-service tool that would offer users recommendations for songs they might enjoy, based on the history of what they have already played, would be a considerable improvement over most current offerings, in which the only way to search for a piece of music that is completely new to you is to browse by genre. Naturally, this would be useful in other media as well as music.

o *Organization*: Very soon, users are likely to have large personal “libraries” of content that they have accessed. New tools are needed that enable users to organize and manage their content; without such tools, their libraries will be as unwieldy as a disorganized directory of email folders. These tools would be enormously useful for all kinds of content, no matter how the users access the content and no matter where the content itself is stored (locally on a portable device, on a server, etc.).

Content delivery:

o *Quality of distribution*: Legitimate content distributors are typically able to offer a higher quality of service than is available in an illegitimate distribution network.

o *Quality of content*: Content in peer-to-peer networks is often poorly sampled, and there is an emerging threat of viruses and spam. Legitimate content can be authenticated in various ways so that consumers would be assured that they only receive official versions of the content on offer.

o *Infrastructure*: Content distributors might arrange new partnerships with infrastructure providers, e.g. with mobile phone providers, to ensure cheap and easy access to content. It would be considerably more difficult for pirates to offer such services.

Business models:

o As suggested above, there is evidence that producers can profit by introducing alternate methods of charging for access to content, including

- 9 -

subscriptions, bundling techniques, and price-discrimination schemes for access to a piece of content at different times or in different formats.7

o In addition to bundling different sorts of offerings of their digital content, providers can link digital content to concert tickets, clothing, club memberships, and other kinds of value-added merchandising.

**6 Conclusion**

We pointed out that unauthorized use and unauthorized acquisition are two aspects of piracy. A key concept is how licenses are bound to content. We saw that various kinds of DRM technology address these issues in very different ways, but that all of them have some kind of flaw that make it highly unlikely that they will be able to solve the problem of piracy. The real problem with piracy is that it takes only a small fraction of users who are capable of dissociating licenses from content to make managed content available to a significant fraction of users in unmanaged form.

We explored the concept of draconian DRM in which devices that handle managed content do not handle unmanaged content at all. Draconian DRM could potentially be effective at eliminating piracy if it were ubiquitously adopted, but introduces a new problem of how to handle public content.

Our conclusion is that currently proposed technical measures will not be able to completely stop the illegitimate distribution of pirated content. We believe that content producers must take steps to compete with the piracy as an alternative.

**References**

[1] E. Allamanche, J. Herre, B. Froba, and M. Cremer, “AudioID: Towards Content-Based Identification of Audio Material”. In Proc. 110th AES Convention, Amsterdam, NL, 2001.

[2] P. Biddle, P. England, M. Peinado, and B. Willman, “The Darknet and the Future of Content Protection”. In *Digital Rights Management: Technological, Economic, Legal and Political Aspects,* ed. Erberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (Springer-Verlag, 2003).

[3] S.A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.S. Wallach, D.

Dean, E. Felton, “Reading between the lines: lessons from the SDMI challenge,” Proceedings of the 10th USENIX Security Symposium, Washington, D.C., August, 2001.

[4] P. C. Fishburn, A. M. Odlyzko, and R. C. Siders, “Fixed fee versus unit pricing for information goods: competition, equilibria, and price wars,” *First Monday*

2(7), July 1997. Available at [http://firstmonday.org](http://firstmonday.org/)/. Definitive version on pp.

7 The pricing of different parts of a sophisticated new offering along these lines might well take into account the risk-management aspects of handling pirates' competing offerings for different pieces of content.

- 10 -

167-189 in *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*, B. Kahin and H. R. Varian, eds., MIT Press, 2000.

[5] <http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp>

[6] <http://www.trustedcomputinggroup.org>

[7] T. Kalker, J.P.M.G. Linnartz, M. van Dijk, "Watermark Estimation through

Detector Analysis," Int. Conf. on Image Processing, ICIP, October 1998, Chicago IL.

[8] F.A.P. Petitcolas. “Watermarking schemes evaluation” IEEE Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000.

[9] C. Shapiro and H. Varian, *Information Rules*, Harvard Business School Press,

1999.

[10] O. Sibert, D. Bernstein and D. Van Wie. “Digibox: A self-protecting container for information commerce,” Proceedings of the 1st USENIX Workshop on Electronic Commerce. New York, New York, July 1995.

[11] H. Varian and R. Roehl, “Circulating Libraries and Video Rental Stores,” *First*

*Monday*, 6(5), May 2001. Available at <http://firstmonday.org/>.

- 11 -

1. Just Cause Avalanche Studio’s talks about PC gaming, video game piracy and DRM http://gamrconnect.vgchartz.com/thread.php?id=126420 [↑](#footnote-ref-1)
2. http://blog.wolfire.com/2010/03/DRM-can-be-effective on effective DRM [↑](#footnote-ref-2)
3. DRM: A necessary evil or a consumer insult? http://www.gamesradar.com/f/drm-necessary-evil-or-consumer-insult/a-20100518133549635045 [↑](#footnote-ref-3)
4. "Gabe Newell on Piracy and the future of the Gaming Industry": http://www.youtube.com/watch?v=pLC\_zZ5fqFk [↑](#footnote-ref-4)
5. "Blizzard: Fighting Piracy with DRM 'A Losing Battle'":

   http://www.shacknews.com/article/64015/blizzard-fighting-piracy-with-drm [↑](#footnote-ref-5)
6. "Ubi DRM: Their side of the Story": http://www.computerandvideogames.com/235596/blog/ubi-drm-their-side-of-the-story/?site=pcg [↑](#footnote-ref-6)
7. Shelf-life being the average time it takes for a video game to “fade out” of popularity, marked by a decrease in sales. Extending shelf-life is often done via Downloadable Content or expansion packs. [↑](#footnote-ref-7)
8. “*Interview with Gabe Newell Regarding Piracy and the Future of Gaming”:* http://www.youtube.com/watch?v=pLC\_zZ5fqFk [↑](#footnote-ref-8)
9. “*Ubi DRM: Their side of the Story”*

   *:*http://www.computerandvideogames.com/235596/blog/ubi-drm-their-side-of-the-story/?site=pcg [↑](#footnote-ref-9)
10. *“Online Poll Regarding Piracy and DRM”* http://forum.suprbay.org/showthread.php?tid=89051 [↑](#footnote-ref-10)
11. “*Online Communications”* http://www.spinproject.org/downloads/onlinecomms.pdf [↑](#footnote-ref-11)
12. "*Official Gears of War 3 Trailer*" http://www.youtube.com/watch?v=n7Te5fcnrUA [↑](#footnote-ref-12)
13. "*CDProjekt RED newsletter: Removal of DRM on The Witcher2:* http://tw2.thewitcher.com/images/newsletter/TW2\_FAQ\_April2011.pdf [↑](#footnote-ref-13)
14. *"What are your thoughts on DRM?":* http://forum.suprbay.org/showthread.php?tid=89051 – A poll on the feeling on DRM, taken from the Pirate Bay [↑](#footnote-ref-14)
15. *“An Interview with Matt Milahy, CEO of Iron Realms Entertainment”* http://www.playnoevil.com/serendipity/index.php?/archives/765-The-World-of-text-MMOs-MUDs-An-Interview-with-Matt-Mihaly,-CEO-of-Iron-Realms-Entertainment.html [↑](#footnote-ref-15)
16. *“Lord of the Rings online profit tripled since free-to-play introduction”:* http://www.gamasutra.com/view/news/32322/Turbine\_Lord\_of\_the\_Rings\_Online\_Revenues\_Tripled\_As\_FreeToPlay\_Game.php [↑](#footnote-ref-16)
17. Free-to-Play refers to games which are essentially free, but offering additional content via micropayments. [↑](#footnote-ref-17)
18. Games which are essentially copies of other, often better-selling games, hoping to achieve sales via copying the premise. [↑](#footnote-ref-18)
19. Micro transactions work best on an initially free product [↑](#footnote-ref-19)