Department of Business and Management
MSc in Management
Course of Digital Innovation

The Effects of Piracy and Counterfeiting in the Video Games Industry

SUPERVISOR
Prof Paolo Spagnoletti

CANDIDATE
Alessandro Piacentini
665731

CO-SUPERVISOR
Prof Maria Isabella Leone

Academic Year 2017/2018
# Contents

Introduction .......................................................................................................................... 4  

CHAPTER I  Video Games Industry Overview .................................................................... 5  
  Brief History of the Video Games Industry ................................................................. 5  
  Present years and future trends ...................................................................................... 7  

CHAPTER II Academic Review ......................................................................................... 15  
  Piracy, Copyright and Digital Rights Management (DRM) ........................................... 15  
    Copyright ..................................................................................................................... 15  
    Legal or business strategy solutions ......................................................................... 21  
    Internet distribution and the P2P system .................................................................. 23  
    Information Hiding ..................................................................................................... 25  
    Policy .......................................................................................................................... 27  
    Summary ..................................................................................................................... 28  
  The Effect of File Sharing on Sales ............................................................................. 29  
    The research on music file sharing .......................................................................... 30  
    Data used for the research ....................................................................................... 32  
    Econometrics and Instruments ............................................................................... 34  
    Findings and Conclusions ........................................................................................ 36  
  Building Efficient Cyberinfrastructures ...................................................................... 40  
    Learning from Cyberinfrastructures ......................................................................... 40  
    Improving cyberinfrastructural practice .................................................................. 41  
    Enhancing resiliency, sustainability and reach ......................................................... 42
CHAPTER III Videogames Piracy and Counterfeiting ................................................................. 44

Origins and development of Piracy ............................................................................................ 44

The History of Game Piracy ........................................................................................................ 45

The Beginnings ............................................................................................................................ 46

Second-Last Consoles generation .............................................................................................. 48

Technical Overview of Piracy ..................................................................................................... 50

The Piracy Threat ......................................................................................................................... 50

Main Piracy Problems ................................................................................................................ 51

Alternative Copyright Protection ................................................................................................. 54

“Almost every gamer is a pirate” ............................................................................................... 54

Always-On DRM ........................................................................................................................ 55

New Issues of the Video Game Industry .................................................................................... 58

The “Game Keys” Grey Market ................................................................................................. 61

Unofficial Online Stores ............................................................................................................ 62

Deep Web and the Black Market ............................................................................................... 65

CHAPTER IV Conclusions .......................................................................................................... 67

References .................................................................................................................................... 71

Table of Figures .......................................................................................................................... 74
Piracy and Counterfeiting are two words deeply linked to markets and economics. In the history of commerce, counterfeiting represented – and still represents – one of the major threats to companies, because the presence of “fake” products on the market leads to an economic damage to those who produce the “genuine” one, and invested money and resources in R&D, quality raw material and marketing.

Piracy, besides the classical figure of robberies and crimes over the Caribbean Sea, is one of the threats of modern economics, concerning digital products and goods, both for professional use or entertainment.

Among the industries damaged by software piracy and counterfeiting, one of the most important in terms of economic value and social relevance is the Video Games industry. Since the beginnings, video game developers and publishers had to face that menace, and the purpose of this essay is to understand how this fight evolved, what solutions were effective and what were not, and why.

Also, it is important to understand what are the real effects of piracy and counterfeiting in the industry of videogames, both negative and positive.

To do this, we will analyze in the first chapter the evolution of the video games market and the evolution of piracy. Then, we will focus on the theoretical solutions proposed by some academic papers and some interesting findings about the effective statistical relationship between piracy and markets. In the third chapter, we will see what solutions have been adopted and what have been their effects, before outlining, in chapter 4, a general model that can be applied to similar industries.
CHAPTER I

Video Games Industry Overview

The Video Games industry works on development, publishing, manufacturing, distribution and retail of electronic gaming devices, software and accessories.

First of all, we identify as the hardware of the computer games industry all the gaming consoles, PCs and mobile devices such as smartphones and tablets: they are the devices that the video game is physically played on.

It is possible to segment the video games industry into two other sectors. Firstly the infrastructure and technology sector, which encompasses the support necessary to distribute and the improved technology offerings needed to play the games; and secondly the software sector, which constitutes the games themselves. Furthermore, within this latter sector, we can find a wide variety of scope of game offerings, such as (but not limited to): Role Playing Games (RPG’s), Mass Multiplayer Online Role Paying Games (MMORPG’s), First Person Shooter Games (FPS) or Platform Level Games (PLG’s).

Brief History of the Video Games Industry1

To better understand the evolution of this industry, it is useful to briefly remind its history2.

In 2005, US President George W. Bush awarded Ralph Baer with the National Medal of Technology by for his contribution to the Video Games.

Working as an electronic engineer for the US Army, Baer was the first, in 1951, to propose the idea of linking televisions to a gaming element. At the time this seemed unfeasible, but after 15 years, in 1966, he was given the opportunity to develop this project. The first interactive game that could be played on a TV screen was released the following year by Baer’s team of engineers.

---

In 1972, during a convention in California, the very first home videogame console was presented: it was called *Magnavox Odyssey*. The following year, Nolan Bushnell founded Atari, a company that quickly gained a dominant position in the market, also thanks to the success of *Pong*, a simple paddle and ball arcade game. Immediately after the market break-through of *Pong*, about 30 videogames have been released in the following two years, from 11 different firms that decided to invest on the development of software to be run by Atari’s console system.

The demand in the video games market started growing faster at that moment, and it was almost 60% greater than it was forecasted to be. By 1983, with a more than 400% increase from the previous year, sales revenues in video games market grew to about $3.2 billion. At this point, with Atari having almost 2/3rd of the US market share, the market became saturated because of the lack of improvements in the offered products.

While the availability of a low cost home computer gave consumers the option to purchase a device with a better technology, with a negative consequence in the market of videogames, Nintendo launched a new console, which would then become a milestone in videogame history: the Nintendo Entertainment System (NES). The Japanese developer also launched Super Mario Bros., that became instantly a successful product because of its high quality and its revolutionary gameplay.

This moment was important since it brought consumers to shift their preference to a good quality product, forcing the videogame industry actors to huge efforts to innovate, especially in terms of graphics. From now on, the videogame market started to be global, with lot of different competitors, both for consoles and home personal computers.

Just 6 years after it was launched, Nintendo's NES doubled its processor and increased its video RAM to 32 times that of its initial version. This exponential growth supports the well-known hypothesis made by Intel’s co-founder Gordon Moore in 1965. In his paper *Electronics*, Moore stated that “the number of components on computer chips will double every eighteen months to two years”\(^3\). This increase in storage capacity available to game developers brought the possibility to offer longer and more complex games, with higher sound quality, better graphic resolution and a sensible increase in the general gameplay longevity.

Throughout the 1980’s Nintendo maintained its dominant position in the video game market, even if as the following decade approached it began facing competitors who finally matched the 16 bit processor standard. A breakthrough arrived in 1994, when Sony released their new console, PlayStation, the first with a 32 bit processor. Nintendo’s answer came two years later, with the Nintendo 64, but Sony’s Playstation 2 (released in 2000) and Microsoft’s Xbox (launched in 2001) marked a huge gap in the gaming console market from now on.

This brief summary of video games history, from the beginning until the new millennium, could highlight how this market has been influenced by the so-called technological leapfrogging4: firstly, Nintendo used the videogame market crash of the early 80’s as an advantage. Then, suffered itself from the launch of highly innovating products by Microsoft and Sony, struggling to recover a relevant position in the home console segment.

Present years and future trends

The video games industry has undergone a total transformation in recent years. Low technology video games, inferior quality consoles, and disconnected users are now things belonging to a remote past. The industry today is at the vanguard of technology and it appears to be a strong market, with good growing rates in the past decade.

Ten years ago, Pricewaterhouse Coopers (PwC) predicted an increase in revenues up to $50 billion within 2012, ranking the video games industry the third fastest growing market in the Entertainment and Media segment. The $100 billion global value of the video game industry has been reached in 20155.

The latest console generation has started to mature, mobile gaming started to grow at a frenetic pace, eSports became really popular, and Virtual Reality approached to the gaming segment with the aim to be the standard for its future.

---

4 Technological leapfrogging is defined as a bypass strategy practiced in high-tech industries: the challenger researches and develops silently the next technology, then suddenly launches it to attack the market leader.
5 http://www.mahesh-vc.com/blog/this-is-the-current-state-of-the-video-game-industry
While in the past decade gamers used to "consume" video games like traditional entertainment contents, nowadays things seems to be changed. This because users today care less about contents created by professionals developers, and enjoy watching other players as well as sharing their own performances and experience.

The incredible growth of eSports and gaming focused streaming platforms like Twitch are part of this trend. As consequence, the games that currently demonstrate to have the most potential have a competitive nature or a large creative user experience. 200 million of people worldwide are expected to tune in as simple viewers at least occasionally; furthermore, about 40% of all eSports spectators do not even play the games themselves. This huge viewership has caused sponsorship contracts and tournament prizes for millions of dollars, forcing companies yet involved in the gaming industries as developers or publishers like Electronic Arts, Microsoft or Activision, but also traditional sport networks like ESPN to create their own eSports leagues and platforms.

In January 2016, indeed, Activision acquired Major League Gaming (MLG), a leader company in the organization of professional gaming circuits and tournament streaming, in a deal worth $46 million: the plan of the video game publisher is, as reported officially, to “become the ESPN of eSports”\(^6\).

In addition to traditional gaming platforms, the sector of mobile games grew up quickly in the very last years, reaching the value of more than one third of the global games industry. Indeed, since mobile gaming can be run on two of the four consumer screen (smartphones and tablets), it wouldn’t be a surprise to see it grow even more in the next future, as well as mobile platforms will overtake traditional platforms such as computers and televisions. Over half of the mobile gaming market is located in the Pacific Asia region, with its 760 million active users representing the 55% of global gamers, followed by North America with about 20%.

A key role is played by China, which digital growth allowed to surpass the US in terms of mobile games revenues last year. The Asian Country has actually a unique mobile ecosystem, as well as its entire internet: mobile apps and games are distributed in a highly fragmented way, with dozens of providers. Furthermore, role-playing games and digital card games seems to be extremely popular in China, with respect to the global mobile market.

---

\(^6\) https://www.theguardian.com/technology/2016/jan/05/activision-acquires-major-league-gaming-esports
When we talk about gaming today, we often refer to mobile devices as well as consoles and to the raise of eSports. Even not so popular in terms of marketing, PC gaming still has a huge share of the total market, both for sales and active users. The PC segment is, in fact, almost as big as mobile, for a value of about $30 billion. Furthermore, much of the professional eSports tournaments take place on PC, as well as the viewership. So that, this platform plays a fundamental role among the gaming environment. Within the PC ecosystem, Steam (created by Valve) has a dominant position, and can be considered the de facto PC games distribution hub. Thanks to data collected by the platform SteamSpy, it is possible to see the size of the PC segment\(^7\). Currently, the total number of active users has reached 260 million of accounts, with an effective activity rate in the last two weeks of about 18% (about 47 million gamers). Each account is supposed to own an average number of games (both digital and physical copy) of 11, for a total of 2.9 million of PC games sold among the Steam platform users – and so almost every PC gamer. Currently, on Valve’s platform database there are nearly 17,000, and Steam services are available in 254 Countries in the World.

\[\text{Figure 1: Total games available on Steam.} \quad \text{Source: Steamspy (www.steampspy.com)}\]

\(^7\)https://steamspy.com/
Concerning the consoles segment, it is important to highlight how the last generation of consoles is extremely focused on the online experience. The market is dominated, as told, by Sony’s PlayStation 4 and Microsoft’s Xbox One, followed in the third position by the former market leader Nintendo. According to IHS Markit, last year Sony captured a total of 57 percent share in console hardware, software and service market, with $19.7 billion of spending by users. The Japanese firm is expected to continue this run until the end of 2017 and after, with a forecast of overall sales of above $20 billion, also thanks to the growth of digital console games.

After an overall console game market reduction at the end of 2016, a positive result has been reached by Nintendo, that officially launched its new hybrid console Switch in March, with a newly competitive position within the so-called console war. In the struggle for the top position, Microsoft is pushing for a rebound from a decline in the last year, focusing on more digital sales and, most of all, on the launch of Xbox One X (codenamed Project Scorpio) as a competitor for Sony’s PS4 Pro in the segment of 4K and 60fps resolution.

At the end of last year, the overall market hit $35 billion in revenues. An installed base of 53 million consoles sold gave Sony almost double of Microsoft’s share, following with 27.6 million.

![World Game Console Market by Platform and by Company](https://venturebeat.com/2017/03/16/sony-dominates-console-market-with-57-share-worldwide/)

**Figure 2: World Game Console Market by Platform and by Company.**

*Source: HIS Markit*
As we can see in the charts, PS4 was responsible for $17.8 billion of sales value, about 51 percent share of the total console hardware market, almost double of Microsoft’s Xbox One at $9.1 billion and a 26 percent share. Nintendo, with its 3DS, was a distant third on the list with $2.6 billion of market value or 8 percent share of the market.

As told, the overall console hardware, software, and services market shrank 2.5 percent to $34.7 billion last year, but the trend for the current year is absolutely positive, with an expected growth of 4.1%, for a total of $36.2 billion. Despite the good launch of its Switch, seems like Nintendo will not reach the results of 2015.

It is important to underline that the drop has been a result of decreased sales volume for console hardware, and a reduction in prices for consoles (including the best sellers). Concerning games contents, the spending in this segment helped to mitigate the decline in hardware spending: both physical media and digital content combined reached sales value of $21.6 billion last year, with a 5.6% increase compared to 2015 results. Also platform subscription played a significant role in sales value, with PlayStation Plus and Xbox Live Gold subscriptions leading to an overall spending of $2.8 billion – up 14% from the previous year.
Nintendo’s console segment has been stable in the last three years, with a 5% share of the digital games content business on consoles last year, nearly $400 million in value. Despite the loss from 2015, due to a lack of new games and paid downloadable content releases, digital spending on Nintendo consoles had a good increase in 2017, also thanks to the launch of Switch, and it is expected to follow this growth trend also during 2018.

Sony and Microsoft, on the other hand, reached significant gains in digital games content spending, considering their whole console offering. In particular, Sony’s business is now worth more than $5 billion, considering only original contents without platform subscription fees.

The top two companies are strongly evolving their digital content monetization strategies: Microsoft recently announced its Xbox Games Pass, while Sony is launching PlayStation Now streaming service.
Those choices are shifting the gaming business to a content streaming business, moving the way consumers deal with contents from owning digital items to gaining the right to use online catalogs for limited periods of time.

Furthermore, gaming industries has starting to introduce the support to Virtual Reality across different segments. In particular, console and PC games developers – as well as console and PC hardware manufacturer – are working hard in order to give consumers a different user experience and being able to contrast the rise of mobile gaming.

Figure 4: Global Games Market in 2017.
Source: Newzoo

To sum up this global gaming market overview, it is important to highlight how current business values and their growth rates are confirming what told before. Mobile games are dominating the market with more than $46 billion, of which $35 billion related to the mere smartphone segment. Console market follows with $33.5 billion, 31% of the total, confirming its loss of preference among overall users. Less than $30 billion is the value of PC gaming industry.
This last one is the only segment of the market with a negative trend, with a growth rate of -2.6%. While console gaming keeps growing at 3.6% (positive result also due to the introduction of VR devices in the last year), the smartphone segment has an extraordinary growth rate of more than 20%, compared to the previous year.

This loss of share by traditional platforms such as PC and consoles highlights how consumers are now prone to a more “casual” approach to gaming, despite the success of eSports events. Gaming industry is now more focused on the distribution of digital only contents than on physical copies and gaming hardware. Also, the introduction of microtransactions and in-game purchases has been at the base of a deal that, in the current year, is worth 42% of the market.
CHAPTER II
Academic Review

Piracy, Copyright and Digital Rights Management (DRM)

Copyright and Digital Rights Management (DRM) have been among the most controversial issues of the digital era. First, it is important to underline that copyright is not a form of censorship. Indeed, while censorship is used to keep information out of the hands of people who are not allowed to know – because of political or social reasons – copyright is a mechanism created to keep information out of the hands of people who have not paid for it. National and International institutions carried out copyright policies such as the DMCA in America and a series of IP Directives in Europe, in order to preserve companies and industries dealing with replicable goods, like music, movies, books and, obviously, videogames.

Through this chapter, we will see how DRM works, before trying to understand why economists point out that stronger DRM would help the platform industry more than the traditional retail industries.

The basic mechanism of Digital Rights Management is to make available an encrypted media file, and then to sell separately a “license” which is the key to the media file. It would be encrypted using a unique code, that the publisher give the user with some statements in a rights management language about what the user itself can do with the purchased content.

Copyright

For years, the protection of copyright has been an obsession of the film, music, book and videogame publishing industries (often referred to collectively by computer industry people as Hollywood). This did not start with the Internet: there were long and disputes in many Countries about whether blank audio/video cassettes, as well as other copy support, should be subjected to a tax whose proceeds would be distributed to copyright owners. This would have been a measure to reduce the losses in revenues due to pirated copies of digital products.

There is a lot we can learn from historical examples such as book publishing, and pay-TVs, but to keep the attention on the videogame industry, we should be looking at software protection.
Indeed, most of the current copyright issues have been played out in the PC and games software markets over the last two decades. Also the music industry contributed to force the computer industry to introduce DRM, arguing that without a proper digital rights management they could go through a lack of revenues. The computer industry replied for years that the music industry should just change its business model, and it could be interesting to use software as the baseline. Furthermore, the computer industry frequently argued in its tussles with the music majors that in an open platform such as the PC it is intrinsically hard to stop people copying bitstreams. Under this last assumption, it is easy to understand that a media file such as almost every digital product is actually very easy to copy.

Softwares to be used on early computers were given away for free by the hardware producers, or released by users who had written them. In the 1960’s, IBM set up a scheme whereby its users could share programs they had written – even if most of those softwares were useless because they were too peculiar, or just too hard to adapt for other users. So that, there was not issues about protecting software copyright. Almost all companies or institutions that owned computers were large and with good incomes, so they could often afford to hire full-time system engineers employed by the hardware vendor on site in order to perform the skilled maintenance required by the software. However, when minicomputers have been launched in the late 1960’s, software costs started to increase significantly. Hardware vendors started to charge extra prices for their operating systems, and third party system companies were founded. At the beginning, they basically offered complete systems to their customers, comprehensive of hardware, software and maintenance; so that, so piracy could not be really an issue. By the mid-1970’s, some of them had turned bespoke systems into packages: software originally written for one purpose would be standardized and sold to customers with similar needs.

In this period, the most common copyright dispute was when a programmer left a company and then joined a competitor: in this way, the competitor could suddenly acquire their codes or part of them, maybe copying some original features. The question then was whether or not it was fair, for a programmer, to bring his knowledge of a code to another company and replicate it.

The standard way adopted to solve such a problem was to check software birthmarks: those birthmarks were features of how a particular implementation was done, like the order in which registers have been pushed and popped.

This continues to be important, and various code comparison tools have been created, oftend developed
by university teams to detect students cheating on programming assignments. This same thread of research has been implemented to detect general plagiarism, by recognizing a passage of text using the least common words which appear in it, in order to index the text itself. So, with time, lots of useful things to do with software started to be invented. For that reason, some system houses started to put in copyright enforcement mechanisms, and common one was to check the processor serial number.

Another anti piracy measure was the one called time bomb: it worked causing a fake error message every few months, saying something like “Fault no. XXXXX. Please call technical support”. The fake error code XXXXX was actually an encrypted version of the license serial number. When the caller claimed to be from a specific customer, the technician would give him a password to re-enable the system for the next few months, while if he figured out it was a pirated copy he would send round a salesman to propose a purchase option.

However, this time bomb mechanism could have been defeated easily if the illegal user understood it and pretended to be an authorized customer. Anyway this mechanism worked fine for several years, with lots of people who encountered the fault message and called the technical offices.

Software piracy really started to become an issue for the computer industry when the market became massive after the launch of microcomputers in the late 1970’s.

In this period, software companies started to produce computer programs that did not need support to install and run them. Consequently, lots of people stated copying and sharing those softwares, without caring about the effects on developer companies and the entire industry. This situation has been clearly described in 1976 by Bill Gates in a famous open letter addressed to computer hobbyists. A year after Microsoft was founded, Gates complained that less than 10% of all microcomputer users had paid them for BASIC. He asked “who cares if the people who worked on it get paid? […] Is this fair?” before concluding that he would be prone to accept the collaboration in his newborn company of any good computer hobbyist: “Nothing would please me more than being able to hire ten programmers and deluge the hobby market with good software”.

---

After those attempts to appeal to people’s sense of fair play, the industry actually changed its approach because of the difference between minis and micros: the latter, in fact, had no processor serial numbers, and it became harder to apply the anti piracy measures issued so far.

---

Figure 5: Bill Gates' open letter to computer hobbyists. February 3, 1976.
There were three new approaches tried: to add a character of uniqueness on to the hardware, to create uniqueness itself in it, or to use whatever uniqueness happened to exist already by chance.

To add hardware uniqueness, as needed to run the first option, it was required the use of a dongle, a device to be attached to the PC’s parallel port and able to answer when interrogated by the software. The most common kind of dongle just had a serial number or were able to execute a simple challenge-response protocol. Some other top-end dongles were instead able to perform some critical part of the computation.

Concerning the second option, a cheaper and widely used strategy was to set up the software in order to make it able to install itself on the PC’s hard disk in a way that could block copy attempts. To make an example, part of the hard disk was marked as “bad” and a critical part of data or of the code has been written on it. If the user tried to copy the product from the hard disk using the utilities provided for the purpose by the operating system, the data hidden in the “bad” sector would not be copied and so the copy would not work. Another example of this option was to require the presence of a customized master disk, made unique by formatting it in a strange way or even burning holes in it with a laser. Generally, though, a distinction was made between protecting the copy and protecting the user: the so-called copy generation control allowed people to make copies in order to have a backup, but it was not possible to make copies of the copies.

The third option was focused on the PC’s configuration, like how much memory, what cards were present, what type of printer. If this setup changed too radically, the software would ask the user to call the technical helpline. This method worked thanks to the vast number of unique identifiers that could be found in the average PC, such as ethernet addresses and serial numbers of disk controllers. With those component details, it could be possible to tie a given software to a given hardware.

However, most of these defenses could be bypassed easily attacking them with a debugger, in order to remove all the protection routines made to the copy by the software. Many computer hobbyists actually did this for sport, challenging each other to be the first to put online unprotected versions of software products as soon as possible after their launch. Even users with licensed copies of the software often downloaded unprotected versions of it, because it could be easier to backup and because those versions were more reliable generally.

Software developers and publishers decided to use also some psychological techniques. The installation routine for many business programs used to show on the screen, maybe on the toolbar, the registered
user’s name and his company on the screen. This would not actually stop a pirate copying and distributing copies registering them in a fictitious name, but this feature would make legitimate users to be less prone to give away their copy of the software to replicate it.

During the late 1980s, the market split up, and the games market moved to of hardware protection. As seen in chapter 1, it ended up dominated by games console products, characterized by closed architectures with their software sold in proprietary cartridges. The reason leading this trend was that consumers tend to be more sensitive about the unit price of a product than about the total cost of ownership, so considering the console itself and all the accessories and games bought during the life cycle of the product.

Thus, the cost of the console was divided and partially distributed between the costs of software and compatible accessories for it. This strategy was implemented for the first time by printer makers, who used to split the cost of the printers and merge part of it within the price of ink cartridges. This also led to strict accessory control that used hardware protection to prevent competitors selling software or other add-ons without paying the relative royalty.

However, software developers generally stopped trying to protect their most popular products using exclusively technical methods, for some of the following reasons.

Unless a producer is prone to invest lot of money on tamper resistant dongle hardware, the mechanisms will be seen as intellectual challenge by skilled and experienced users, whom will put efforts to publish unprotected code as soon as possible. So that, code that is not protected would not have this challenging character.

Whit processors becoming faster, operating system interfaces becoming higher level and codes becoming more complex, software protection routines – like the ”bad disk sector” one – becomes harder to write as a consequence. The effect on both protection and piracy is an increase in the costs and the technical complexity.

Furthermore, when multiple protection dongles are used, they could even interfere with each other. Those software protection techniques could make a product less strong, causing problems to the users, maybe when they have to recover from backup to a new hard disk. Moreover, protection mechanisms could also cause software from different developers to be incompatible and, in lot of cases, unable to be installed on the same machine.
With time, technical support became more and more important, because software products became more complex; obviously, only customers that paid for the software could receive it.
Also, the arrival of computer viruses was a great thing for the computer industry itself. This because they forced customers to invest in software security, which meant that casual copying could not be done so easily. Within the following years, antivirus programs made it harder for copy protection programmers to create efficient software for the purpose, because non-standard operating system usage could set off virus alarms.

Is it important to underline that part of the users often made only a casual use of the product, and so they would not be actually prone to spend money for it. In this sense, we can say that a certain level of piracy was good for business. In fact, people who use a pirate copy of a certain software – and they try it just because they do not have to pay before using it – could like it, and often decide to buy a regular copy and also persuade other people to buy one.

Another common issue in software protection mechanism has been related to the fact that many developers preferred not to have to worry about whether the software was licensed to the user – and could decide to use it on a new machine – or to the machine – and could sell the machine second-hand with the software still installed on it.
As both cases were very common, software protection mechanisms that made them much harder could often cause problems to users and mechanisms like the use of dongles, that could easily deal with both, were quite expensive, either for implementing and support costs.

Legal or business strategy solutions

The developers then decided to move to legal solutions. One of the first main initiatives was to establish anti-piracy trade organizations within the most involved Countries, like the Software Publishers’ Association in the USA. The first legal actions have been moved towards some large companies that allowed (or endorsed) the widespread diffusion of pirate software. Then, hundreds of small and medium developers have been forced to officially clarify their positions on copyright policy, with the threat of random controls by the designated authority.
Concerning the fight against anonymous software copy makers, some tricks were used to get pirates to incriminate themselves. A typical one was the so-called salted list: generally, a list of fake companies with phone numbers directed to the publisher’s helpline, whose staff would ask for the caller’s
company and check if it is on the list of paid subscribers. Software industry eventually discovered that the law provides tools for enforcement, but sets also limits to that.

The above described time bombs technique has been found to be illegal in a lot of jurisdictions. For instance, in 1993, the director of an English software company received a criminal conviction under Britain’s Computer Misuse Act for “making an unauthorized modification to a system”, because they just used a time bomb to force the payment of an invoice. After this judgment, other legal systems began considering time bombs unacceptable, unless the customer has been adequately notified of their existence at the time of purchase.

Then, the attention moved back to technical mechanisms. Site license agreements are carried out by license servers, which are actually similar to physical dongles. This license agreement mechanism started to be implemented on PCs belonging to a corporate network, and could apply a limit to the number of copies of an application allowed to run simultaneously. Actually, the network license server could be defeated easily by disassembling the application code, but this became harder as code became larger; furthermore, the threat of a legal action to preserve the copyright started to be combined to those security and anti-piracy measures. Thus, we can see that the software industry decided to combine technical and legal measures, since both have their limits in different ways. From a managerial point of view, a certain number of copied products started to be accepted, with the purpose of leveraging them with a minimum threshold of fully-paid sales.

Then, emphasis was given onto online registration. Indeed, designing a digital product so that users are forced to interact with the developer web site – for instance, to download malware signatures for an anti-virus software, rather than a security patch or real time data such as the latest exchange rates – it is possible for the developer itself to keep a log of everyone who uses the software. It’s also worth noting that different methods are used to counter different threats. Is possible to detect large-scale commercial counterfeiting by monitoring the serial number of a specific product that has been registered online; however, such operations are found and closed down by using investigative agencies to track products back through the supply chains.

One exceptional case can be applied to huge companies, which have a big disposable income. The option is to provide not just the software but also a processor able to run it. It does not matter that software-as-a-service may be the ultimate copyright protection or DRM for software nor any other content that can be used exclusively online. For the user it would not be possible to buy it, rather than freeze the software version he is running or use it offline.
Except for the case described above, none of the protection technologies available mass-market can be considered foolproof, especially against a determined opponent.

However, by using the right combination of those technologies, a large software company can often get an acceptable result, especially if it keeps prices not too high by comparison to the market average and if has a good reputation among users.

In this sense, small software companies are instead under less pressure, because their products tend to be more peculiar and the risk of becoming a victim of piracy is lower. So that, they can often get away with making little effort (or even none at all!) to prevent copying and piracy. Furthermore, if they have only a few customers, it may even be worth for them to supply software-as-a-service.

There are also other alternative business models. One example is to give away a demo version of the product, and sell online a password in order to unlock its complete features. A radical variation of the model consists in giving away a completely free version of the software, and then make money just from selling software-related services.

This experience has led many insiders to believe that the solution for Hollywood’s problem lies in a change of the business model.

**Internet distribution and the P2P system**

During the mid-1990s, a number of researchers started to work on solutions to control the sale and distribution of digital goods over the Internet to consumers owning a personal computer. The original projects concerned the distribution of newspapers and articles from journals and magazines, since the distribution of music and video files would request more network bandwidth.

The basic problem was that a PC, being a general-purpose machine, has been also designed to be able to copy any file and send it to any other computer. Unlike analogic copies, digital ones are perfect, so millions of copies can be easily made from one original.

This feature cannot be properly defined as a problem but, from the content distributor point of view, every PC owner is the “enemy”. The music industry believed that unlimited copying would be the cause of the destruction of their business, but the computer industry replied that digital rights management was intrinsically impossible on a general-purpose computer such as the PC, so the definitive solution would have been a new business model.
Furthermore, the music and film industries had much more influence on the policy makers, despite they were a tenth of the computer industry’s size, and the result was a number of products generally referred to as digital rights management or DRM.

Despite the diatribe between computer people and Hollywood during the 1990s – about whether DRM was possible or desirable – years later it seemed that both of them have been taking the wrong position in the argument. Indeed, stronger DRM turned out to benefit more the platform vendors than the content developer companies.

During the following decade, peer-to-peer file-sharing has become one of the main ways in which music/video files were illegally distributed online. The idea, born within the world of censorship-resistant systems, was to set up networks with no central node, so it was technically impossible to close down the pillars of the system itself using legal attacks.

The first massive use of this illegal distribution system has been carried out by Napster, which enabled people to share MP3 audio files with each other. In order to avoid legal actions, Napster just provided an index of available files, so that a user wanting a given track could find out who else had it, rather than keeping the files centrally. The platform attracted tens of millions of users, but in 2001 legal representatives of the industry found a way to force it to close down.

However, other peer-to-peer networks, such as Gnutella and Freenet, quickly filled the gap left behind. Those networks were in turn inspired by the earlier censorship resistant systems, and were followed by more “commercial” systems like eMule. Once again, industry lawyers suddenly targeted them and, besides legal actions, also psychological strategies were now attempted, giving those systems the reputation of being full of spyware.

The United States Copyright Office defined peer-to-peer networks as “networks where computers are linked to one another directly rather than through a central server”\footnote{Anderson, R., Security Engineering, (p. 708)}. The absence of a central server that could be closed down after a legal action created an interesting problem for music industry, as well for every other industry dealing with digital products. As told, they also tried psychological persuasion, pulling out voices about the danger of sharing all the hard disk of a PC by using a P2P software, rather than just sharing selected files such as music tracks.

The point of strength of peer-to-peer networks was that they are made of well-connected nodes, each of them can be independently connected to every other.

In file sharing systems, every node corresponds to a different user, and most of them actually contribute
more than their share of the uploaded files. This is an interesting feature of the peer-to-peer system, that contributed to the creation of one of the most innovative systems of the last decade: the blockchain and the cryptocurrencies.

On the technical-countermeasures side, music industries firms were also working to spam out systems by uploading damaged music files – which may be not properly fair, but is for sure legal – but they were also suspected of carrying out denial-of-service attacks – which, on the contrary, is illegal in many jurisdictions. However, there was no evidence of those last actions.

**Information Hiding**

In the mid-1990’s, with military’s interest in unobtrusive communications and public concerns over government efforts to control cryptography, digital product industries started to find new ways to protect copyright. The attention moved to the development of new techniques of information hiding. Confidential information were hidden within other data, such as when in an MP3 audio file has been hidden a secret message, or the serial number of a software embedded in the order in which certain instructions should be executed.

The purpose of digital products developers was to use some copyright marks that could be hidden in digital audio, video and artwork in an unobtrusive way. These specific marks are generally either *watermarks* – which are hidden copyright messages – or *fingerprints* – which are hidden serial numbers.

Steganography represents an interest in total privacy, since the purpose of its techniques is to embed a message (that should be kept secret) in some cover medium in such a way that it remains undetectable. However, a copyright mark has no reason to be “secret”, because the need for uniqueness of a digital license is easily understandable and, most of all is a right. For this reason, copyright marks do not actually require to be hidden in order to be effective. TV channels represent a clear example: they usually embed their logo in a visible but unobtrusive manner in the corner of the picture. Furthermore, many DRM systems have control tags bundled quite visibly with the content. In most of cases this is the appropriate technology, but for what that concerns software and videogames, we should focus on hidden copyright marks.

The success of DVDs was followed by the concern about the so-called “analog hole”, which was the possibility to decode digital and audio media files into analog format, and then convert them back to
the digital version, in order to copy and distribute them without any trace of copyright bypass. For this reason, they set out to invent a copy generation management system, which could work even with analog signals. The basic concept was to set a video or music track as unmarked, or marked “never copy”, or even marked “copy once only”. Users were not allowed to record a video if it was marked “never copy”, and after recording a video marked “copy once only” it would be changed to “never copy”.

While commercially sold media contents would be marked “never copy”, broadcast contents such as TV shows would be marked “copy once only”, in order to let consumers to copy them with their home devices. This feature allowed personal DVD players to copy home videos unlimitedly, avoiding TV video piracy at the same time.

The mechanisms was based on hiding one or more copyright marks in the content. For each copy there was a ticket X, which included a random number, copy control information and some unique information to the physical support. Then, using a one-way hash function \( h \) was possible to compute \( h(X) \) and \( h(h(X))^{11} \). This latter was the actual hidden copyright mark to be embed in the file. Compliant machines were set to look for a watermark, and once they find one they would refuse to play the protected file they are supplied with \( h(X) \), which has to be checked by hashing it and comparing it with the mark.

Things were finally arranged so that a device could only record a marked track if given X, in which case only a \( h(X) \) was written to the new support. In this way, a “copy once only” file in the original medium became a “copy no more” file in the new medium. Companies belonging to the Secure Digital Music Initiative (SDMI) decided to adopt a fragile watermark, which would be damaged by unauthorized processing.

Furthermore, the introduction of Self-Protecting Digital Content (SPDC) processors allowed to embed unique fingerprints into decrypted content in real time. Each plaintext\(^{12}\) copy of a video derived from a decoder could be unique, and it was possible to use forensic techniques to determine which device it

\(^{11}\) A hash function takes a group of characters (called a key) and maps it to a value of a certain length, called hash. The hash value is representative of the original string of characters, but is normally smaller than the original. Hashing is used in encryption or in database indexing because it is easier to find the shorter hash value than the longer string.

\(^{12}\) Plaintext usually refers to unencrypted information pending into cryptographic algorithms. It should not be confused with cleartext, which refers to data that is transmitted or stored unencrypted (“in the clear”).
came from – unless the device itself was corrupted, so that it was not possible to identify the user who leaked the file.

Information hiding has even more ancient roots than cryptology and cryptography, going back to the wars between the Greeks and the Persians.

Also Francis Bacon could be considered a pioneer of DRM, since he proposed a system to embed binary messages in a text: one bit per letter, by alternating between two different fonts.

As told above, being able to hide a security message or a unique code is much more important than enciphering it for copyright protection purposes. The modern terminology adopted in this subject defines that the copyright mark or embedded text (in the case of steganography) should be hidden within the cover-text and produce the marked text (or stego-text). Additional information are often added, called marking key (or stego-key), and it can be used to recover the mark or embedded text. Obviously, the word “text” can be replaced by “video”, “audio” or any other appropriate term.

Policy

The Intellectual Property policy debate became a very discussed subject between the 1990s and the early 2000s, when a series of laws from copyright term extension to America’s Digital Millennium Copyright Act (DMCA) gave much more power to the owners of the intellectual properties themselves, such as copyrights, trademarks and patents holders. As a consequence of this shift of power, many people involved in the computer industry could be threatening.

Furthermore, the DMCA gave copyright owners the power to force Internet Service Providers to take down those websites that published some infringing material – the so-called Notice and Take Down power. In addition, stated by the Notice and Put Back power, has been set for the subscribers of some copyright violating content a term of 14 days to send a counter notice and give all the infringing stuff back; otherwise, the copyright owner could sue the subscriber. In many cases, ISPs would actually just terminate a customer’s service rather than getting involved in legal disputes.

In addition to legal controls there were also access controls, and many legal scholars criticized this kind of privilege, since it could create a new bundle of de-facto rights, that experts used to call “paracopyright”.


At the same time, millions of people suddenly became aware of copyright law: while it was only a concern of specialists such as publishers in the past, it now involves everyone who downloads music or administrate a personal web page. Since the law has failed in keeping up with technology, a wide gap has been created between what people are allowed to do and what they actually do.

This law-norm gap is expected to become wider, because we are increasingly moving to a “remix culture”\(^{13}\), and as the many minor infringements are now easily and suddenly going online, despite they usually take place in private – or unidentified public – spaces. On the other hand, we must also consider privacy concerns. In the past, people would buy physical copies of books, movies and music albums; moving to a digital copy market, dealing with a huge number of downloads means that DRM license servers keep a record of what people watch and listen to, how often they do it and from which geographical location.

**Summary**

To sum up on Ross Anderson’s paper about copyright and DRM, we can assume that protecting a digital content against illegal copying represents a hard problem, both technically and politically. Under the technical aspect, it is difficult because personal computers can copy almost any without any cost; on the other hand, it is politically difficult because of the collateral damages made during the attempts to impose digital rights management on the reluctant computer industry. Even though some of the problems people were thinking about did not actually happen — like, for instance, the effects on reverse engineering for compatibility — there is still real complexity. Compatibility between DRM systems represents a big issue on the technical level, also because it is not completely clear how DRM will work in the near future, when people will expect to play digital contents that they have purchased on multiple devices.

\(^{13}\) Anderson, R., *Security Engineering*, (p. 719)
Concerning the political level, it seems that the digital entertainment industry has damaged itself by shifting power in the supply chain from itself to the platform vendors, in order to try to obtain a stronger DRM level.

The development of copyright and digital rights-management systems over the last decade has been exponential, and its further evolution seems to follow the same trend. In this sense, there are many interesting research problems in copyright management, like better ways of embedding copyright marks in digital contents or the production of cheaper tamper-proof hardware tokens.

The Effect of File Sharing on Sales

As we have seen above, there is an intense debate between industries dealing with any kind of software or entertainment content about the appropriate level of protection for intellectual property. Since its first diffusion, the Internet has been a natural benchmark to understand the consequences of reduced protection, because of the drastic reduction of the cost of copying information. In their paper, Oberholzer-Gee and Strumpf analyzed whether illegal file sharing has reduced the legal sales of music contents. They have been the first, in 2007, to put concretely the attention on the phenomenon and to study it starting from actual data about music files downloads. This is interesting for essentially two reasons. The first is that the results of the study can be compared to gaming contents and the whole gaming industry market value, as described in the first chapter. The second reason is that illegal music file piracy and counterfeiting has been the very first step to the piracy of bigger and more complex digital products, like professional software or videogames.

Reading the results of the paper, it seems that the effect of downloads on sales is statistically indistinguishable from zero. Indeed, the estimates of the study have been valued inconsistent with claims that file sharing is the primary reason for the decreasing trend sales of music albums, according to the data gathered during the period of research.

---

The research on music file sharing

As told in the previous paragraphs, file sharing has become one of the most common online activities right after the mass diffusion of the Internet. Since physical distance among users is irrelevant for the purpose of file sharing, people from almost every country in the world can take part in the stream. In the United States, the amount of shared files among private users was of about 300 million each month, with a growth rate of over 50 percent in the last two years.\(^{15}\)

The authors defined file sharing as a “largely nonrivalrous” practice, because the owner can retain the original copy of any downloaded file, and the key reason for the growth of the phenomenon has to be found in the low cost of sharing and significant network externalities.

When Napster was founded, in 1999, pioneering the practice of decentralized file sharing through P2P, few users actually used to take part regularly. Then, in 2006, the number of simultaneous users on the major peer-to-peer networks reached 10 million.

The great interest in understanding the economic effects of file sharing has been emphasized by the music industry itself, after quickly blaming this phenomenon for the decline in sales. In the 5 year prior to the research (so between 2000 and 2005) the number of music albums sold in the United States had a loss of 25 percent. For this reason, recording industry started suing thousands of individuals who used to share files, claiming that this practice was the main offender. The Supreme Court was asked to rule on the legality of file-sharing services, because among the new technologies it was the most harmful for the markets. In the meanwhile, the Congress started considering a number of measures in order to counter the perceived threat of file sharing.

While there are widespread concerns about peer-to-peer, the theoretical effect of file sharing on music sales and profits has still an ambiguous nature. Indeed, users could get confused and substitute downloads for legal purchases. Such substitution can maybe be limited by the low quality of downloaded files and the lack of premium features. Moreover, illegal file sharing allows users to try products they would not otherwise be exposed to if they had to pay for. Among P2P user community, it is common practice to take a look to each other’s files library, and eventually discuss about albums and artists in specific chat rooms or forums. This experience exchange can indirectly promote new sales, with a benefic effect on the industry.

---

\(^{15}\) Data referred to 2007, when the paper has been published.
On the other hand, a different theoretical approach seems to have unclear effects on sales. Indeed, users can use file sharing to sample music, which will result in an increase or decrease of sales depending on user’s personal preferences. The availability of file sharing could also influence the willingness to pay for music: it could decrease it because of the possibility of free download, but also increase it because of network effects.

Furthermore, it is possible that there is little effect on sales. This because sharing a file lowers the price of the file itself, moving those users that are not so interested in purchased to change their mind thanks to the price cut-off.

Without any prediction based on a theoretical formula, the effect of file sharing on sales was just an empirical problem with no clear solution. We cannot accept the entertainment industry’s opposition to file sharing as an a priori evidence that the file sharing phenomenon leads to economic damages. Indeed, so far the industry itself has blocked new technologies in many occasion, claiming that they could bring damages; however, those technologies became often a source of profit for the whole industry. General surveys are the source of most of what has been reported about the effects of file sharing, but evidence is often mixed.

In order to avoid this unclear conclusion on the effect of piracy, the study used observations of actual file-sharing behavior of a large population rather than data gathered from surveys. The collected data set included 1.75 million file transfers, the 0.01 percent of total download starting from the last third of 2002.

Audio downloads of users in the United States have been matched to a representative set of commercially relevant albums, creating a database of over 10,000 album-weeks, to directly study the relationship between downloads and sales.

The results of the research were that file sharing has had only a limited effect on record sales, the estimated effect of file sharing on sales was not statistically distinguishable from zero, and also the economic effect of the point estimates was small. The authors estimated that file sharing cost the industry no more than 24.1 million albums per year, that is 3 percent of sales (and less than 1/3 of the decline observed in 2002).

It is interesting to underline that while downloads occur on a huge scale, most users are often individuals who in the absence of the opportunity of downloading the music files for free would not have bought the same music they downloaded. Furthermore, while the main estimates focus on high-
frequency variation over several months, the experiments focused on long-term trends using data spanning several years.

The results of Oberholzer-Gee’s and Strumpf’s research also have broader implications beyond the specific case of file sharing. Indeed, the level of protection for intellectual property that is necessary to ensure innovation has been a long-standing question in economics. The paper provided a specific evidence on the impact of weaker property rights for the case of music industry, but the model can be adapted to understand how the file-sharing technology available across the Internet era had markedly lowered the protection that copyrighted products enjoyed. It is interesting to analyze this reduced protection adversely affected sales, extending this assumption to every industry dealing with copyrights and intellectual properties.

**Data used for the research**

Data collected for the research have been extracted from the log files generated by download servers. Those information, of which most users are actually unaware, are the main data set for the analysis. Researchers focused on downloads because those are the files that users actually obtain, and they can potentially displace sales. The analysis was restricted to audio files by users in the United States, identified by the Internet protocol addresses (IP) included in the server logs.

An important question was whether the sample was representative of data on all P2P networks. Authors figured out that the availability of titles is highly correlated on the networks. Using a standard homogeneity test based on 1,789 unique songs, they could not reject a null that the download samples were drawn from the same population. Individuals in data gathered for the paper are similar to those on the most popular networks because the user experience is quite similar, and many individuals employ software that allows them to participate simultaneously in several networks.

Furthermore, has been figured out that users on these larger networks and those on observed servers had access to a comparable number of files and that network size had just little effect on the distribution of downloads.
The sample used for the study is representative of all commercially relevant albums, and it allowed to draw meaningful inferences about P2P’s effect on overall album sales.

The average album in the resulting sample sold 143,096 copies during the study period, and across all categories, 44 percent of population sales are represented in the sample. Using a two-sample Kolmogorov-Smirnov test to compare the distribution of sales on the original charts and in the studied sample, the researchers were unable to reject the null that sample sales are representative of the population of all albums (p = 0.991). They also rejected this null comparing each of the original charts with the sample sales for that particular chart (p > 0.539 for all charts).

In order to compare sales and downloads, the 260,889 songs that U.S. users successfully transferred during the study period have been matched to the 10,271 songs on the 680 albums in the sample. The matching procedure was hierarchical in that each transfer line was analyzed, identifying text strings that could be artist names. Then, those strings have been compared to the artist names the data set. Once the artist was identified, text strings were then matched to the set of songs performed by that particular artist. The algorithm matched 47,709 downloads in the server log files to the list of songs, with matching rate of about 0.18.

The researchers identified two reasons why that rate is less than 100%. First, a downloaded song may not be in the sample, and this is not of any concern, since it simply reflects the fact that the analysis has done on a sample.

The second reason for a match rate of less than 100 percent could be attributed to a failure of the matching algorithm. To estimate the failure rate, part of the sample has been hand-checked, resulting in a range that confirms 18% as a rate that reflects the truth.

Observing the dataset used for the research, the first fact that appears evident is that the file sharing phenomenon has a global nature. Indeed, even if over 90 percent of users are based in developed countries, with the US leading with 31%, among the whole dataset a total of 150 countries are represented.

Furthermore, there is only a loose correlation between user share and other country covariates such as Internet use or the software piracy rate. The fact that interactions among file sharers transcend geography and language is confirmed by the 45% download rate by US users that receive their files from other U.S. users, with the remaining 55% coming from a diverse range of countries, including Germany (16.5%), Canada (7%), and Italy (6%).
While file-sharing activities were geographically dispersed, the authors figured out that only a limited number of songs were actually transferred with any frequency. Indeed, among the sample, the average downloads number for a single song was 4.6, but the median number was zero. Even if the sample was representative of the most commercially relevant music of the period, more than 60 percent of the songs have been never downloaded.

Up to the album level, has been observed that users made 70 downloads from the average album. The most popular album among P2P users had about 1,800 downloads, whereas the median number was just 16, the 75th percentile was 63, the 90th percentile was 195, and the 95th percentile was 328. Comparing those download statistics to the ones referred to sales, it was possible to observe that both (downloads and sales) were closely following a Pareto distribution (power-law).

Considering the low cost of sharing and sampling music on P2P, what could be expected from P2P users is the choice to download a great variety of songs, from many different musical styles. Actually, the list of P2P downloads closely resembled the play lists of top 40 radio stations. So that, it is not surprising that songs from best seller albums were downloaded more frequently.

Concerning sales, in the top quartile of the rankings albums average 200 downloads, while in the bottom part the mean number of downloads was only 11. This fact suggested that downloads and sales are driven by common factors, highlighting a key concern for the development of the empirical strategy of the research.

**Econometrics and Instruments**

As told, the goal of the research was to measure the effect of file sharing on sales. The authors observed sales and downloads at the album-week level for a period of 17 weeks. These data allowed them to estimate a model with album fixed effects, described by the following formula:

\[ S_{it} = X_{it} \beta + \gamma D_{it} + \omega s + v_i + \mu_{it} \]

where \( i \) indicates the album, \( t \) denotes time in weeks, \( S_{it} \) is observed sales, \( X_{it} \) is a vector of time-varying album characteristics that includes a measure of the title’s popularity in the United States, \( D_{it} \) is the number of downloads for all songs on an album, and \( \omega \) controls for time trends (a flexible polynomial or week fixed effects).
The key concern in the empirical work was that the number of downloads was likely to be correlated with unobserved album-level heterogeneity.

As the above mentioned statistics suggested, the popularity of an album is likely to drive both file sharing and sales, implying that the parameter of interest $\gamma$ will be estimated with a positive bias. The fixed effects $\nu_i$ imperfectly control for some aspects of popularity, due to sudden changes over the entire study period.

The authors address this issue by instrumenting for $D_t$ in a two-stage least-squares model. Furthermore, instruments $Z_{it}$ predict file sharing but are uncorrelated with the second-stage error $\mu_{it}$.

Since correlation between prices and unobserved product quality represents a problem, the researchers decided to use cost shifters to break the link between unobserved popularity, sales and downloads. The main advantage of those instruments was that they do not rely on the common assumption that product characteristics are exogenous.

The analysis presumed that each instrument influenced download costs and that those costs affected the number of file transfers. By analyzing server log files, the authors have been able to calculate the download time and success rate of download attempts. So, download costs have been classified into five different measures:

- the time between a download request and the successful initiation of the download ($C_1$);
- the time between a search request and a download request ($C_2$);
- the time between the initiation of the download and its successful completion ($C_3$);
- the ratio of search requests to the number of successful downloads ($C_4$);
- the percentage of failed or canceled download requests ($C_5$).

Each $C_i$ term captures aspects of delay or frustration that the typical user might experience.

It is important to underline that generally there were long delays for top-selling albums, that is the evidence of a worldwide lack of download supply in the first period, a great advantage to legal sales. In this sense, misspellings plays a key role, significantly increasing the time between a search and a download request as well as the number of unfulfilled downloads ($C_2$, $C_4$, and $C_5$), while its effect on the time it takes to transfer a file ($C_1$ and $C_3$) is not consistent. Even if misspellings do not actually slow down the file transfer, we can conclude that they contribute to create confusion in relation to the subject of the research.
By the way, estimated effects on download times are economically significant. In the specific, those results were considered meaningful only if the cost of downloading had an influence on the number of file transfers. This fact could not be obviously true because P2P users are often running other activities while files are being downloaded, with a big influence on the time cost of file sharing. So that, the authors estimated the following system to check whether the variation in download time that was due to the used instruments had a significant impact on the number of transfers:

\[ C_{it} = Z_{it}\delta + \nu_i + \mu_{it} \]

\[ D_{it} = C_{it} + \nu_i + \epsilon_{it} \]

where \( Z_{it} \) is the full list of instruments and \( C_{it} \) denotes total download time \((C_1 + C_2 + C_3)\). What results evident is that P2P users are sensitive to the time cost of file sharing: indeed, a one-standard-deviation increase in download time leads to a reduction of downloads by almost half of their mean. Furthermore, for each of the five \( C_i \) terms have been found similar effects in the second equation of the system when estimated separately.

Those estimates confirmed the initial claims of the authors, that attributed to external and random factors the source of influence on costs of downloading. For instance, they figured out that German vacations periods can have a sensible effect on the number of downloads in the United States.

Findings and Conclusions

To analyze the findings of the research, it is useful to look at the following graph (Figure 2)\(^{16}\). It plots the weekly time series of sales and downloads for one of the most popular albums in the sample. The best seller album was actually ignored in P2P networks until its worldwide availability for sale in the 10\(^{th}\) week. This highlights the influence of the official release that leads sales as well as downloads.

Furthermore, the quick but different decays in sales and downloads underline the importance of the use of high-frequency data for the analysis.

![Figure 6: Dynamics of sales and downloads for a popular album. Period expressed by week, sales and downloads in thousands.](image)

A dynamic analysis model allow only for a contemporaneous effect of downloads on sales, but there might be the possibility that downloads influence sales at a later point in time. Indeed, users could like some of the music that they downloaded, and consider to purchase it in the future.

A possible explanation for the inability to find a statistically significant relationship between file sharing and sales is that people who share files and consumers who legally purchase music actually belong to two separate groups. In this sense, file sharing growth should displace sales, but is not possible to identify that effect because data used for the analysis were not enough to reflect properly the increasing number of file sharers.

The authors found out three answers to this conjecture.
The first one was that it was inconsistent with the known consumer behavior. Indeed, while it could be easy to think that people who share files no longer buy CDs, the results of many surveys told that they actually continue to purchase legal albums.

Second, considering the growth in file sharing, it was possible to find a displacement effect because of the dropout replacement of purchases with transfers. So that, the number of downloads in the sample has been scaled in order to match the growth in file sharing.

Finally, a third approach was to compare the long-run sales growth of individual genres of music.

At the end of their study, the authors figured out that file sharing had no statistically significant effect on purchases of the average album. Indeed, a one-standard-deviation increase in file sharing reduced an album’s weekly sales by just 368 units, and the statistical effect was too small to be distinguished from zero.

Since the sample was fully representative of the population of commercially relevant albums, it was possible to estimate the effects of peer-to-peer file sharing on the entire industry, and a null hypothesis ($H_0$) that the decline in sales was greater than 24.1 million units has been rejected. Furthermore, the estimates become more precise assuming that P2P affected only simultaneous sales and allowing for growth in the number of file sharing users. After those further estimates, the conclusion was that the impact in sales could affect a maximum of 6 million albums; so that, during the research period (2002), the impact on global sales has been of just 0.7% of purchases.

Since file sharing could not be the main reason of the decline in music industry sales, the authors stated that the change in how music was distributed and the ending of an atypical high sales period were the actual main reasons of the phenomenon.

More important, for the purpose of this paper, is the reflection that the authors made on the trend of the whole entertainment industry. Indeed, in those years the level of competition among different forms and products for entertainment started to grow exponentially. A big shift toward movies was accounted in the closely previous years (both DVDs and some of the last VHS tapes), with an increase of more than $5$ billion. Consumers start also to spend more on video games than in the previous decades, increasing by 40% in the same period, as we have seen in the details in the previous chapter.
Also, in this period mobile phones tripled their diffusion, and the mobile content industry would have been born shortly thereafter.

The authors were aware of the fact that those results represented a trend wider than it appeared. Indeed, they successfully predicted that those results would hold in the following years, also thanks to the incoming technologies. This brought to a key question: how social welfare would change with weaker property rights for information goods?

On the basis of the results, it wasn’t consistent that file sharing had a significant effect on the supply of recorded music. The effect documented have been too small to change the amount and the quality of recordings that artists who produce commercially relevant products have released. Concerning new artists and bands that are launching their career, probabilities of having success and having a virtually zero income are at the same low level.

The authors, finally, agreed with Rob and Waldfogel\(^\text{17}\) in arguing that file sharing likely increases aggregate welfare. Indeed, the limited shifts from sales to downloads can be simply considered as transfers between firms and consumers, and the dimension of peer-to-peer activity suggests that file sharing adds high levels of social welfare.

Building Efficient Cyberinfrastructures

In this final part of the chapter, we will go through some brief concepts about cyberinfrastructures, in order to figure out what are the main characteristics and what could be the issues related to them. This is useful to understand what could be the weaknesses of a complex infrastructure like a digital retail system, and how to deal with such complex systems to make them more efficient. For this purpose, a good choice is the paper *Understanding Infrastructure: Dynamics, Tensions and Design*, in which the authors summarized some recommendations to better implement an existing cyberinfrastructure starting from what they observed and learned in the 3-days workshop host by National Science Foundation in September 2006.

Learning from Cyberinfrastructures

First, the authors focused on how to learn from existing infrastructures, in order to allow growing ones to develop themselves in a more efficient way.

A comparative social scientific analysis of the large number of cyberinfrastructure projects that are currently proceeding in parallel, paying attention to their handling of social, cultural, and organizational issues and completed by high-level requirements analysis, could be useful in developing programmatic principles for future projects. Indeed, it would extend, deepen, and generalize from the limited social scientific studies of cyberinfrastructure that have been conducted so far.

A cross-agency and cross-national comparison could also be useful for this learning purpose. A broader comparison with workshops and other similar initiatives hosted by federal funders and national funding agencies should also be supported in order to extend the effective case set of cyberinfrastructure studies. The best result could be achieved, in this sense, if multinational teams of researchers will use common research questions, methods, and protocols.

The authors noticed the need for a more accurate and realistic reporting mechanisms. This because, looking at the anecdotal evidence from many of the workshop participants, it is clear that there is a tendency to over-report experiences of success and under-report those of difficulty or failure. Encouraging the honest reporting of failure would result in a more scientific approach, useful to deeply analyze and understand cyberinfrastructures dynamics.

---

As many cyberinfrastructure experts pointed out, the current reward system in the academy does not provide incentives to scientists, researchers, students, or administrators to contribute to activities based on this subject. Indeed, every activity involved in cyberinfrastructure development tends to be really intensive in terms of time and effort, but they often go unrecognized when contributing to the value of research activities. The proposed solutions are basically two. First, providing specific provisions for the preparation, sharing, and distribution of data, and second, to work with institutions to legitimate cyberinfrastructure-building activities as rewardable academic work. Combining these two strategies, with an accurate framework of requirements and the creation or encouragement of reward structures for meeting these requirements, could shift academic culture toward the right support for cyberinfrastructure studies.

Additionally, it is possible to enhance the learning mechanism by instrumenting cyberinfrastructure projects for the purpose of a social scientific analysis. This could be obtained, for instance, including provisions for retention of project-related communications and sampling interviews across the range and duration of specific projects. In this sense, every cyberinfrastructure project would benefit from the inclusion of social scientists on project teams.

**Improving cyberinfrastructural practice**

The authors then found some strategies to enhance training and improve the quality of cyberinfrastructure projects.

First, they noticed that a capacity for in-process analyses could become a regular part of the working routine of cyberinfrastructure experts. Being more sensible to the dynamics and tensions of cyberinfrastructures and being able to see these early on could support in-course corrections, contributing to efficacy, relevance, and sustainability of the project.

Then, they highlighted the importance of training for information managers, which occupy a strategic, under-recognized, and hard to fill spot in the contemporary research environment. Information managers represent the human articulation between domain-specific demands and needs, and the emerging opportunities and constraints of cyberinfrastructure. They cover often also the role of principal keepers, curators, and coordinators of data, and, for this reason, their figure deserves a specific training course.

Furthermore, cross-disciplinary symposia for graduate students and post-docs could produce a common focus on shared experiences, problems, skill sets, and application potentials for cyberinfrastructure.
Finally, the authors underlined the necessity to fit funding to time scales. Indeed, there is often mismatch between the long time horizons at which large-scale infrastructures have historically developed and the typically much shorter ones of cyberinfrastructures programs and projects (typically 1-5 years).

**Enhancing resiliency, sustainability and reach**

Finally, the authors suggested strategies useful to enhance flexibility and extend the reach of the cyberinfrastructure. First, they focused on the need for a design of the cyberinfrastructure easy to adapt for flexibility and change. Indeed, given the quickly changing technological environment and the relative immaturity of the infrastructure itself, managers and administrators should support efforts “not to prematurely sink or fix the form and vision of cyberinfrastructure”\(^\text{19}\). Is important to underline that resiliency is often a feature that can be fundamental in almost every ecosystem to face drastic changes. In fact, as we have seen in detail through the history of counterpiracy evolution, only companies capable to understand how their industry and system were changing have been actually able to contrast the threat of piracy through the evolution of their business framework. The authors have identified three dimensions at which a company dealing with this kind of infrastructure should assess:
- disciplinary representation;
- actor type and scale;
- form, mechanism and timescale of investment.

The second feature needed is a continued and expanded mechanism able to incorporate under-represented institutions and groups. This is important in order to let everyone involved in the development of the cyberinfrastructure to collaborate and participate equally. Finally, to avoid redundant expertise, it is important to form alliances with experienced niche organizations. For instance, part of the expertise that is not part of the core research could be found outside the usual academic channels, and this could help not to waste time, efforts and resources in such side research. In other words, it is way more efficient and easier to capitalize on other expert’s experience through targeted partnerships.

---

A good example of this involves licensing and intellectual property management issues that are common to almost every industry and environment. For this purpose, a wide number of projects offer open intellectual property databases, like The Creative Commons, Scholar’s Copyright Project or Science Commons.
Origins and development of Piracy

Videogames can be defined as the core of a cultural innovation, since they have been, in the last decades, one of the main product concerned in the development of the so called “information economy”. What we have seen in the previous paragraph is also that, in the last years, the online experience has become the core feature of the gaming products, both on traditional gaming platforms and on new portable devices. In particular, videogames are playing a main role in the smartphone and tablet revolution, collecting millions of new casual gamers that are, actually, completely new to gaming. Furthermore, concerning console and PC gaming, videogames are pioneering the use of high-intensity cloud computing, due to the high technical requirements of the latest product and the powerful servers needed to host huge number of players in the same match.

In this way, videogames industry has an exponential level of innovation that few other industries can demonstrate, and most of them are still connected to the gaming sector.

It is also important to highlight that game industry has a high level of development of original and creative content: it is offering lot of new innovative ways to enjoy its products, involving consumers in the online experience more than any other content industry currently does.

Videogames industry embodies technological innovation, thriving on the development of original intellectual property for all the games and series released every year. This continuing success is, inevitably, also due to a robust and workable IP framework.

In this paragraph we will go through one of the main issues related to the industry of gaming: the problem of piracy and the black market of counterfeited gaming products.
The History of Game Piracy

Videogames can be classified as a form of intellectual property, as well as books or movies. Once a videogame is created it can be copied infinitely, like every other software or file, and this is what made gaming industry vulnerable to piracy since its dawn.

Copying a game has always been a cheap practice, because the copier devices and hardware are making no contribution to the cost of making the game itself. However, the really negative consequence of this behavior is – as a general rule for every kind of business – that if every consumer copied or purchased a counterfeited copy of the game instead of buying it there would be no revenues for games developers and, so, there would be no future games business.

We can classify game piracy into two main forms. The first one is the individual game player piracy. In the past, games were often copied using physical media, but since the diffusion of the Internet it has been possible to share online copied and counterfeited games. The second is commercial counterfeiting, where a professional criminal community manufactures games, partially – and almost totally – copying existing official products.

Profiling games piracy on different platforms always give different results, because of the variety of technology used, the demographics of the users, the market size and trends at different given times, relative costs (maybe related to the single developer or publisher itself), and a number of other external factors. What can be easily assumed is that when piracy takes hold on a platform, many hundreds of thousands – and sometimes million – of copies of a videogame are made in a short range of time.

Videogame piracy can be defined as a huge scale theft, which deprives the developer and publisher companies of big amounts of legitimate incomes, harming the whole videogame development industry as an obvious consequence.

From an economic point of view, it is not possible to say that every pirated game copy is actually a lost sale. In this sense, we can recall the simple price elasticity of demand to understand that, at a lower price, far more units of the product would be consumed than a higher price per unit.

Nevertheless, this economic statement cannot be used as an apology for piracy and counterfeiting, since the lose of potential sales by games publishers is at the same lever of an indirect cost raised independently from the company’s business.

---

The Beginnings

The first mass market game devices used to have a tape interface. For that reason, games and softwares were sold in audio compact cassettes. From a technical point of view, those magnetic tape media were very easy to copy, especially after dual cassette players started to be popular and became cheaper. As soon as copying proliferated on a massive scale, it started to hurt game publishers. Consequently, many of them went suddenly out of business, or were forced into mergers in order to survive.

A whole range of technical anti-piracy solution were introduced and one of the first was called Lenslok\(^21\). This latter used a row of micro prisms in order to split a code to be displayed on the screen, like a sort of optical coding-decoding. Because of its simple nature, it has been quite easy to bypass this software protection, and it has been defeated by software crackers after a few months of usage. The huge trouble of these technical solutions would have not been faced by game publishers if copying had not been a great threat to their business. At first, they also attempted an economic solution, releasing budget games at low prices, at which they were not worth copying.

Despite the good response of the market to those budget games, lot of game publishers went bankrupt in the early 80’s, because when piracy took off seriously, general sales came to an abrupt halt.

In this period, British publisher *Ultimate Play The Game* (then became *Rare* and acquired by Microsoft) was one of the most highly regarded publisher for 8 bit home computers. Badly affected by piracy, Ultimate’s response to the drop off in sales was to raise prices from £5 to £10. The logic behind that choice was that if customers paid more for a game, they would be for sure less inclined to give away their games to be copied an indefinite number of times by a third person – and so to be the only one to pay in a vast group of users.

As easily expected, this strategy did not work, and after a year the company decided to switch the attention to the Nintendo Entertainment System (NES), which did not suffer from piracy at that time, and some other main publisher took the same decision. So that, 8 bit computer owners lost out heavily as publishers put less and less resources into developing for their machine or quit entirely, as Ultimate Play The Game actually did.

After the launch of Commodore Amiga and Atari ST, copying became technically easy once again, and it expanded quickly. This time, publishers understood it was up to them to find technical solutions, and a true technology war broke out between game software developers and the pirates.

\(^{21}\) https://www.wikipedia.org/wiki/Lenslok
The second step of anti-piracy measures has been the use of random texts printed on the game manual: sequences of letters and digits with no logical meaning were used as activation codes. This led to a huge amount of photocopying by the pirates, and so publishers decided to start using photocopy proof manuals. As a side effect, those efforts against piracy made revenue generation very difficult, forcing game publishers to struggle in order to survive like it was an industry crisis. Indeed, lot of companies admitted piracy was one of the reasons for the downfall of the early game machines market.

After this period, as told before, Sega and Nintendo emerged in the market of video games. Their consoles were running games held on chips inside special cartridges, so it was technically difficult and expensive to copy them. This did not allowed piracy to have the massive extent that it had on early gaming platforms like Spectrum or Amiga, and so the game industry could finally arise to the level we all know, with many great titles and franchises becoming popular worldwide.

By the way, cartridges were expensive to make, so eventually the hardware manufacturers returned to recordable media, in order to make vastly larger games with far lower production costs. The first company to move in this direction, in 1995, was Sony, which used CD-ROMs to load games on its PlayStation. The Japanese manufacturer used several anti-piracy measures which protected it from piracy for years; however, with the diffusion of modchips and the development of PC CD-ROM burners that could burn data in the same way that the PlayStation used to, piracy became again a concrete threat. Games sales started collapsing again, with pirates selling copied games privately or through organized black market networks.

Games publishers were again in troubles, and the number of released products shrunk dramatically. In 1999 the industry released 100 titles, the following year the number of published games was 78, while in 2001 just 33 games has been launched. Since the PlayStation remained in production until 2006, the collapse of software publishing just halfway through its sales life is a clear sign that piracy started again to be heavily influent.

In 1998 Sega launched the Dreamcast, using a special unique disk format called GD-ROM. Once the disk was circumvented with hardware like the Utopia bootdisk, it was irreparably corrupted, and the owner couldn’t use it anymore.

However, pirates found out quickly a way to avoid this technical measure, and condemned the Dreamcast to die just after a couple of years, with more than 10 million of sold units. This also condemned Dreamcast’s manufacturer, Sega, to leave the console hardware market, causing to the industry the loss of a great publisher that played a main role in the past years.
Concerning PC industry, after the diffusion of internet, home machines have been connected in massive numbers. This played as an advantage for games industry as well as for piracy. One of the first PC game to be massively pirated has been *Severance Blade of Darkness*, published by Codemasters. This game was really popular, and among users was built an active community of mod makers. Yet Codemasters sold very few copies of the game, because most people just downloaded it for free from the internet.

So the game developer, *Rebel Act*, received very little royalties and was forced to leave the business. In the following years, it appeared virtually impossible to viably publish boxed PC games, because most of them appeared on the internet as free bit torrents before they were even in the shops. Once again, it was far quicker and easier to pirate a game than it is to buy it. This forced most publishers to give up, even those with a decades long tradition in PC games. In 2008, *Reflexive*’s director of marketing Russell Carroll reported his company suffered from a piracy rate of 92%, and this same rate could be probably the average of the whole industry. When publishers tightened up their protection in order to preserve their business it didn’t help much, because people just moved on to some of the many other games that are available for free by bit torrent.

Also, in 2008 Electronic Arts started releasing PC games for free, with their development cost supported by in game advertising and micro payments. This settled a new trend in video games industry, that revolutionized the whole business, both for security and for user experience. Furthermore, another solution started in this period to make PC games as a viable business has been to make online games (MMOs), because these are server based and so impossible to pirate.

**Second-Last Consoles generation**

The PlayStation Portable (PSP) has been a very popular mobile gaming machine and media player made by Sony. They have sold 33 million and has represented a graveyard for games publishers. It has been hacked since its early life, and it was simple to copy games onto and find every game very easily available for free online. So that, most developers just did not invest millions into AAA games for it, because they would be wasting their money. This lack of quality games on the PSP (obviously along with some other factors) left the door open for

---

the Nintendo DS to become a massive success with 70 million sold.

But even Nintendo’s portable console has been pirated soon, using flash memory cards in dummy cartridges. This impacted heavily on DS game sales and led publishers to become reluctant to develop for it, as they were with every heavily pirated platform.

The last generations of home consoles, the Microsoft Xbox 360, the Sony PlayStation 3 and the Nintendo Wii, gave a strong effort in the war against piracy. All three machines had good technical anti piracy measures. Nintendo went so far as to embed a secret second CPU (an ARM) in the graphics chip to run some of its system software (they lost $975 million to piracy in 2007\(^24\)). However, all three have been cracked (not fully with the PS3) and owners were able to bypass the anti piracy and play free games.

In the meantime Nintendo started making successive popular game releases that looked to see if the machine has been modified before they will play. If it had, the Wii becomes a “brick” for that game. Microsoft started using Xbox Live to look for modified 360s and cancel the accounts of any that they find.

Sony had the advantage that Blu-ray media was expensive to buy and difficult to copy.

\(^{24}\) https://www.bit-tech.net/news/gaming/nintendo_lost_975_million_to_piracy_last_year/1/
Technical Overview of Piracy

The Piracy Threat

The major threat to the videogames industry is represented by piracy. It costs every year hundreds of millions of Dollars, due to the lost sales.

In recent years the Internet has played a vital role for the industry, being the main driver in the rapid growth and development of online games, leading to increased game development, production and jobs. The growth of online piracy, however, has been a major hindrance and discouragement to the provision and take-up of online game services, as well as being highly damaging to traditional physical goods business models. Online piracy causes widespread economic damage to European game developers, publishers, distributors and retailers. It also hurts national tax revenues and undermines the prospects for economic growth, employment and technological innovation.

It can take two to three years and tens of millions of euros to bring a major game title to market. Only a small percentage of these games achieves profitability, and the active sales cycle of a new game release is often only a few months long. The industry, therefore, incurs particular damage due to the widespread availability of devices and software designed to circumvent the technological protection measures (TPMs) that the industry uses to protect its games. This affects companies of all sizes, damaging both revenue streams and employment levels right across the industry.

To combat piracy, the game industry has tended to rely, first and foremost, on its ability to invest in the development and introduction of disruptive technologies and business models, rather than on litigation. Experiences with new business models, however, tell us that with new approaches, new IP and related enforcement challenges also emerge. These new threats may not be entirely IP infringement based, but may instead resemble acts of fraud, theft or misappropriation of services. While new business models are clearly part of the solution to piracy, and they are being aggressively pursued, they are not likely to be complete answers, in and of themselves.

---

Main Piracy Problems

**Hosting and Linking Sites**: Hosting sites store infringing files uploaded by users that are then made available for download by other users. Linking sites feature one-click links to these stored files. The wholesale use of links to further and facilitate the downloading of pirated content by millions of users worldwide has become an enormous problem for all of the content industries, including the game industry. The links are posted by users who are generally “members” of, or affiliated with, the sites concerned and are usually organised by content category and/or supported by search functionality to facilitate users finding the content they are seeking.

The linking sites have a business model consisting of deliberately and systematically making infringing game and other content available through the provision of links, and they generate profits by running ads that monetize the high volume of visitor traffic attracted to the easy access to content that they provide. The operators of both hosting and linking sites can generate substantial revenues from advertising (and from subscription fees or donations as well), and they generally operate anonymously and without respect for local taxation or other laws. They are also very adept at hopping from one hosting provider to another, whether in the same country or in another. Despite industry efforts to take down millions of infringing game files and links, they persist as a significant source of pirate game downloads.

**BitTorrent Indexing Sites and Trackers**: BitTorrent indexing sites serve a similar function to linking sites. However, rather than directing users to hosting sites, indexing sites provide users with links to torrent files, which enable them to connect with other users to share infringing game and other content. These sites (the largest and most notorious of which is, of course, The Pirate Bay), therefore, serve a primary function of enabling users to find torrents for infringing copies of game files, permitting them to find and join swarms where such copies can be downloaded from the other peers in the swarm, using a BitTorrent application.

BitTorrent trackers are servers that facilitate transfers between peers using the BitTorrent protocol. They play an indispensable role in directing the traffic of users who are attempting to participate in the P2P transfer of content via BitTorrent. Trackers facilitate and expedite the creation and growth of swarms, and thus the infringing copying and downloading of illegal copies.
Like the other content industries, the game industry suffers serious economic damage from widespread illicit P2P file-sharing. The casual infringements regularly committed by millions of users worldwide are an example of what has been rightly termed by an English High Court Judge, as “the tyranny of small decisions that have ruinous economic consequences”.

*Circumvention Device Distribution Sites:* Some e-commerce websites are dedicated to the sale of devices (such as “mod chips” or “game copiers”) or software (“soft mods”) that bypass the TPMs that the industry uses in its consoles and handheld devices to protect its games. By enabling users to download and use infringing copies of games, the distribution of these devices contributes to a higher level of game piracy. Device or soft mod sites may distribute directly to the consumer, or furnish raw materials to online or physical services that install such devices, i.e. circumvention services. Nine out of ten of the most popular (by traffic ranking) e-commerce sites that offer circumvention devices for sale within the EU are hosted and operated from Spain.

Day-by-day, these circumvention devices further fuel the levels of online piracy because each one functions as a gateway to multiple future infringements and inflicts untold damage on legitimate game sales. The widespread availability of circumvention devices and services significantly contributes to the growth of online piracy, as unauthorised copies of games downloaded from the Internet can only be played on consoles modified by such devices, technologies or services.

*Unauthorised Private Servers (also known as “pirate servers”, “grey shards”, “emulators”, or “black net servers”):* Among the most popular of the new online business models in the game industry are the “free-to-play” (F2P) and, particularly among MMO (Massively Multiplayer Online) games, the monthly subscription model. The cloud-based nature of F2P and subscription based games clearly insulates companies from some of the traditional strains of online piracy. Because F2P games are distributed free of charge, and because much of an MMOG’s value derives from server-based action, the harm associated with unauthorised copying and distribution of client software is diminished. However, new forms of piracy designed to exploit cloud-based content services have emerged in recent years. One particular threat involves the establishment and operation of unauthorised private servers that are used to host unauthorised game play. These servers seek to replicate the functionality of a publisher’s official server, allowing users to play an online game without connecting to that official
server. When users are diverted to play on unauthorised servers, the publishers are not able to monetise their online games (through advertising, microtransactions, or monthly subscriptions), and thus face reduced opportunities to recoup their investments.

Establishing and maintaining unauthorised servers often involves multiple acts of copyright infringement as well as the circumvention of TPMs. When cloud-based games are distributed, the publisher typically incorporates into the client software TPMs that prevent the client from connecting to servers other than those operated by the publisher. Operators of unauthorised servers must therefore distribute either hacked versions of the publisher’s client software or circumvention software designed to disable the client’s TPMs that would otherwise prevent the client from connecting to the unauthorised server. Moreover, to enable online gameplay, operators of unauthorised servers must often use infringing copies of a publisher’s server software.

Game companies’ terms of service generally prohibit gameplay on unauthorised servers, and publishers generally try to add features to their official servers to make the gray ones less attractive. As the game industry migrates to cloud-based distribution models, it is unfortunately likely that the unauthorised server phenomenon will begin to supplant more traditional forms of piracy.

**Unauthorised markets for digital entitlements**: F2P, “freemium”, and MMO games in which the sale and attainment of digital entitlements (in-game currency, play enhancements, achievement-based rewards, supplemental game content) are central to the game experience, are frequently undermined by unauthorised secondary marketplaces that offer these entitlements for sale in exchange for real-world money. In many cases, these digital or virtual goods are themselves copyrighted artwork and images. In nearly all cases, publishers’ EULAs and terms of use prohibit the sale of such items outside of their games. The sellers in these unauthorised marketplaces often acquire these digital goods by employing phishing schemes and other fraudulent conduct to steal player accounts and to empty them of the player’s hard-earned goods. These unauthorised markets destroy the carefully-calibrated in-game economies necessary to promote a good player experience, and ultimately undermine the value of the games themselves.
Alternative Copyright Protection

After the analysis of the phenomenon under its more technical aspects, it is useful to focus on the point of view of a company involved in the struggle of counter-piracy management. As we have seen, through the decades of videogames history there have been continuous technical gap filling strategies on both sides – companies and pirates. Indeed, every time a company managed to put a new intellectual property protection system in their products or devices, pirates figured out how to bypass them; again, companies developed new systems and pirates finally jailbreaked them too, and so on. So that, this whole story could be told like a never-ending race between “good” and “evil” IT engineers.

For that reason, videogames industry developed the idea that the solution could not be merely technological, but it need to be mostly managerial. Changing the way gamers play games, forcing every copy of a game to show its license ID to control servers and sensitize customers to avoid illegal products would be the features of this kind of solution.

“Almost every gamer is a pirate”.

In 2012, Ubisoft’s management declared that, from the data owned by the company, it was fair to admit that just one in ten PC gamers legitimately bought games, This could be seen as a justification for a move towards more free-to-play and web browser-based titles.

Actually, the French software publisher had its attention put on growing its PC market share, but kept insisting that one of the only way forward was to offer games completely for free. The reason behind was the creation of better and more advanced in-game items as a new strategy to face the piracy threat. Indeed, in a note released by Ubisoft’s founder and CEO Yves Guillemot, was clarified that between five and seven per cent of free-to-play gamers on the PC platform would fork out for in-game content.

However, Guillemot also alleged that as for its regular PC games, only about 5% to 7% of users pay anyway. He claimed the vast majority apparently was running a pirated copy: "It's around a 93 to 95 per cent piracy rate, so it ends up at about the same percentage as free-to-play".26

26 Retrieved at [www.theregister.co.uk/2012/08/22/ubisoft_says_over_90_per_cent_of_pc_gamers_are_pirates/](http://www.theregister.co.uk/2012/08/22/ubisoft_says_over_90_per_cent_of_pc_gamers_are_pirates/), visited on January, 08th 2018.
Since the beginning of the Internet era, Ubisoft gained notoriety for its always-connected DRM measures, a method of piracy prevention that deeply influences the concept and the structure of the game, and creates new trends in the videogame industry. Indeed, given the high piracy rates and the failures of mere technical counter measures, a great number of publishers started to adopt this different business model, changing their relations with and the wider gaming community as a result.

Yet in June 2012, at E3 (Electronic Entertainment Expo), Crytek’s CEO Cevat Yerli revealed his company’s plans to go all out free-to-play (F2P) for future games releases – an effort to contrast the well-documented piracy problems that the publisher suffers from.

The quality of F2P gaming usually leaves a lot to be desired not only in storyline, but also in terms of the advantages paying for extras can deliver that makes the gameplay unfair for its users. The problem of piracy affects all content providers, so developers have been forced to deal with inventive ways that allow their business to survive.

**Always-On DRM**

While the online music industry decided to shift away from utilizing DRM, the video game industry continues to employ restrictive DRM technologies. Even though these two industries are certainly not identical, video game companies had actually a lot to learn from the decisions took by the major music labels over the years, since music industry suffered from the consequences of piracy for a longer time, as we have seen in the previous sections of this paper. Over the past ten years, the major music labels have agreed to leave DRM restrictions of digital songs sold through online music stores. This because DRM has proven to be an unsuccessful strategy for the online music industry, failing in stopping songs piracy and driving away honest consumers by frustrating them with the lack of control over legally purchased music content. So that, the decision to eliminate DRM restrictions was well received by consumers, with an increasing trend in online music purchasing.

However, the most important companies of the video games industry decided not to adopt this concept: indeed, the most important games franchises released in the last years are featured by a new form of DRM protection called “always-online DRM”, that in some cases seems to be frustrating for most part of the users.
Always-online DRM is a method that requires a user to be online at all times, in order for the game to run. On the one hand, this allows video game companies to combat piracy by periodically checking that a user is a valid one. On the other, this can create a truly dissatisfying gaming experience for those consumers who have legitimately purchased a gaming title. For instance, if a user is playing a game in single player mode, which does not require an internet connection, he could actually be booted from the match and lose the progress he has made while he was playing if the internet connection happens to go out. A game reviewer once complained about that, stating that even without losing the connection, “the spectre of catastrophe hung over [his] head like a razor sharp guillotine”.

Even worse, if a user happens to be somewhere that lacks internet service, he simply cannot play the game at all.

While always-online DRM might make sense in some future world in which an internet connection is available everywhere with constant reliability, this is clearly not the case today. Instead, always-online DRM punishes the very consumers who are keeping video game companies in business, those who have legally purchased the games. This approach to DRM, which holds fighting privacy above the gameplay experience of consumers, has proven to be incredibly damaging in the past.

To report an example, we can think about Spore, a game that was released by Electronic Arts in late 2008 with DRM restrictions that prevented users from installing the game on more than three devices. In addition, Spore required users to verify that their copy was legitimate each and every time they went online. For this reasons, users became so frustrated with such a highly restrictive DRM system that pirated copies became the most popular, bringing Spore at the top of the list of most pirated games for the year 2008.

Like the other solutions adopted through the years, always-on DRM seems to be inefficient because it has a strong side effect on the experience of legal consumers. While doing away with DRM protection entirely may not make sense for the video game industry, keeping consumers satisfied must be prioritized above and beyond fighting those who violate copyrights. Otherwise, once-loyal customers may decide to use pirated copies.

Tommy Refenes, known for being the developer of Super Meat Boy, declared that piracy cannot actually be stopped.

---

He argued that piracy is a fact of the modern gaming industry, but that it is ultimately not harmful, and that digital rights management is just the worst thing that can be done in the attempt to prevent it; instead, respecting players is the best way to attract new customers and make them loyal.

As described, the new dominant trend in the industry is a mix of online gameplay and always-on DRM. Different developers use very different methods to control the losses that can result from game piracy and it is hard to figure out whether or not they can be actually efficient, or which of them works better than the other. Refenes founded imperfections in this way of thinking:

“The reality is the fight against piracy equates to spending time and money combating a loss that cannot be quantified. Everyone needs to accept that piracy cannot be stopped and loss prevention is not a concept that can be applied to the digital world. Developers should focus on their paying customers and stop wasting time and money on non-paying customers. Respect your customers and they may in turn respect your efforts enough to purchase your game instead of pirating it.”

What that the developer argues is that piracy, unlike refunds, does not properly represents a lost sale. Indeed, DRM hits customers that the company knows are paying for their game, and it risks turning those actual sales into lost sales. Invasive DRM practices bring apathy rather than excitement, and excitement is the best way to sell games in any sort of market. If customers feel too disappointed with a game or a franchise, they would not care about it in the future and the general willingness to buy products from a specific publisher may dramatically go down. Those arguments are difficult to justify to large companies, because it is surely hard to get past the concept that pirates are stealing games, and that it's a bad thing. Anyway, it might be possible to see, not so late, a shift in the way that developers view piracy. Reportedly, even the director of HBO’s popular show Game of Thrones admitted that illegal downloads do not matter and might have an upside, even though he has to recant its declaration after.

So that, after years of trying to control piracy, maybe companies will finally just start to allow for it.

---

New Issues of the Video Game Industry

In the recent years, Video Games industry changed its strategy, following the possibilities introduced by latest technological support. In particular, there has been, as seen, a massive switch towards online based gaming. This offers of course a new scenario, both for the fight against piracy and the competition among developers and publishers. Despite this thriving trend for the whole industry, it seems that a lot of emerging practices may cause the sudden decline of the entire video game market, as reported by Robert Brockway in 2013. The journalist found out four main issues that, in his opinion, represent the real menace for the industry of gaming.

1. **Persistent Connectivity**
   As described, the new gaming industry trend is to have a persistent connection to the game servers. This can be bothering to users, because some of them cannot always have Internet connection, and some others may not have a connection at all (i.e. those who live in rural areas). This discriminates people who do not care about the online multiplayer features and just want to enjoy their games in a single player offline mode. Furthermore, sometimes users have to face the opposite problem. Indeed, for those who have a connection and do want to play online with other people, the problem can be related to the weak connection of the game servers. Online based games require more technical support than offline ones, because servers have to handle millions of simultaneous connections, across different systems and countries, at all times for the whole life cycle of the product itself.

2. **Microtransactions**
   In order to increase the revenues from a game – even though they are not influenced by the distribution of counterfeit copies – publishers begin to insert some in-game purchases, varying from a few cents to tens of dollars. Sometimes this does not influence the quality of the game, because the objects that could be unlocked are just “beauty accessories” for a character or a weapon; so, those who play the game with this kind of premium accessories would just have some fancy customizations. Notwithstanding, premium features are often more than aesthetic features, giving a big help to the user who bought them.

---

This will have a consequence for both those who pay and those who do not. Indeed, the users that play the game with a “power-up” can easily get bored of such kind of experience, without a challenge. This can be translated in a shorter life cycle of the product, which loses its ability to attract the user for a less amount of hours.

On the other hand, the skill gap that is made in a multiplayer match may bother people who do not pay for additional features. This pay-to-win formula makes a game less attractive, because virtually forces people to pay more just to have a fair challenge. So, buying a basic version of the game would mean being the weaker fighter inside the arena.

Microtransactions are now part of some of the most important gaming franchises, and even though they are a big source of revenues, they are also moving the consumers’ attention towards games from competitor publishers who decided not to adopt such a business model for their products.

3. **Wait Gaming**

The third issue identified by Brockway involves a new category of games, *wait games*. This category is often used by the so-called casual gamers, those individuals that do not take gaming so seriously and use to play browser games and, more often, mobile games, just to fill some minutes of spare time, like a 10-minutes break at work.

Wait gaming works this way: the user downloads a free (or even sometimes a cheap pay) game, and at first it will allow him so many rounds, minutes, or lives. Then, when the player runs out, a countdown pops up, and it is not possible to play again until it expires. Of course, users could always just pay to bypass the waiting.

The author then asks what is so wrong with the wait gaming model. This is not so bad when it is a free game. It is possible to take a well-known mobile game as an example: Candy Crush Saga. It is so addictive, and people pay nothing to start it. A few cents to unlock some features or to have additional attempts might seems it worth it. Users get tens of hours of gameplay out of it, and ultimately pay much less for the experience than they would for a full-price PC or Console game. Every user would be right to think that if it stopped there, but it doesn't.

Indeed, wait gaming is now leaking into pay games. Mobile games now have a cost of only a few dollars, when they have any free basic version. There are microtransaction stores, but users can avoid them.
The only wait gaming occurs when players buy new objects or weapons: then they have to sit for a variable number of real-time minutes or, more often, hours before the object purchased is actually available. This does not happen if the user decides to pay some game currency – gold, diamond, coins or whatever they call it). Those virtual coins can be bought with real money, and users often forgot they already paid for the game. This new trend is contributing, according to many expert of the game industry, to the lack of interest in gaming that can suddenly cut of part of the revenues.

4. Third-Party DRM

The last point involves all the environment of invasive third-party DRM. Brockway’s critic start from gaming consoles, because by their very nature, consoles themselves represent a type of DRM. Every console uses its own architecture and its own formats to lock the games to that device and this represents the most basic form of electronic security. The user is already giving up a little bit of ownership by agreeing that this separate product, the game, is only for use in conjunction with this other product, the console. It is not like a DVD player, because it is proprietary, and so it is DRM. Furthermore, consoles then started introducing more restrictions and penalties like persistent connectivity, online passes or no used game trading.

Concerning PC gaming, Steam is a fine example of a DRM platform. Indeed, in addition to its own security measures, Steam also allows developers to launch their own services or platforms. Examples of that could be Uplay for Ubisoft, Origin for Electronic or Games for Windows Live. Often, it is mandatory to sign into developer’s servers or create a profile before users can launch the game for the first time. In other words, sometimes users are launching a DRM service that launches other DRM services inside of it, and there is no technical reason for it.

The journalist then concludes his article claiming that developers will never stop piracy.

He Brockway points out that DRM measures have failed in fighting piracy in the past, but piracy levels are just the same they have been before. The solution proposed is not giving a strong and meticulous control for every user – just because they are “potentially pirates” – but giving more attention to customers’ tastes and needs. “Worry about the customers you do have” – he says – “or you won't have them anymore”. 
The “Game Keys” Grey Market

We have seen how the development of online features in videogames have created the possibility to implement a new way to fight piracy or counterfeiting of gaming software. Indeed, online based games allow publishers to control the licenses of every user connected to the servers, and block those who are using a counterfeited copy. The same happens for single player offline based games that offer several updates, and so require often to be logged into official servers. So, unlike past years, in the last decades publishers found out a way to “look inside” every PC or console that is running their products, simply exploiting the availability of stable and fast Internet connection of almost every consumer.

Among the other important innovations brought by the wide diffusion of good – or almost decent – Internet connections, there’s been the increasing volume of the digital retail market. The main reason why consumers appreciated digital copies of a video game is the availability of the purchases at any time and everywhere: they only need a connection and a console or a PC to access their own “digital library”. Even though consumers cannot get rid of their old games by selling the discs, the possibility of changing their hardware without losing their progresses, saves and achievements makes gaming much more worth than the past.

The purchases can be made directly paying on the retailer’s website with a credit card or other digital payment method, or redeeming the product using a univocal alphanumeric code (game key) previously bought. Then, the game will be forever linked to the account.

Furthermore, when two or more accounts are logged into a console, it is possible for the one that have bought a game to share it with the others which haven’t. That last feature actually represents a gap in the above-described always-on DRM, and seems that piracy has been able to take advantage of that. Indeed, traditional piracy switched to online grey market at the same time as the official market switched to the online retail business model.
Unofficial Online Stores

During the last decade, a lot of online platforms dealing with game keys or game accounts have been created, and between them we can identify as the more important G2A, Instant Gaming, Kinguin and AllKeyShop (even though this last is actually a search engine). Those websites gained a good reputation among users, because they actually sell what they declare – game keys or accounts credentials owning a particular game in its library at a cheaper price than the official stores.

Before going further with the analysis of such unofficial online stores, it could be useful to give a brief definition of what is defined as grey market.

A grey market is “a market employing irregular but not illegal methods; especially, a market that legally circumvents authorized channels of distribution to sell goods at prices lower than those intended by the manufacturer” 31

It is important here to focus on the keyword “legally”. Indeed, those platforms are usually confused with black markets, but the actual point of strength of unofficial retailers is exactly their non-illegality. Most of people think getting game keys from G2A, Instant Gaming, Kinguin or any other resellers is illegal, but, by definition, buying a game key from a grey market key shop does not make the customer a pirate or a partner in crime.

As told, grey markets circumvent authorized channels of distribution by getting their products from secondhand sources. Flea markets and stores dealing with used games like Gamestop are examples of grey markets, as well as online secondhand market platforms like eBay or Amazon.

Purchasing a product gives the buyer full ownership of that product: it belongs to him/her, to use as he wishes. This is an irrevocably understood truth that digital media has been struggling with for decades, and what grey markets exploit to offer their competitive prices.

So, starting from a neutral position about unofficial retailers, is important to figure out where do the keys come from. Some journalists investigated on that, identifying five different categories of game codes 32 33.

First of all, the developers themselves. As some of the grey market platform clarify in their FAQ sections, anyone but the developer can generate key codes for a specific game or software.

Each time a key is made, developers can cite the intended distribution point of it. Platforms like Instant Gaming, G2A, AllKeyShop and Kinguin are commonly used, so they are usually part of the distributor drop down list. That clearly and officially means that developers can and do choose to sell keys on those sites. From an economic point of view, the reason behind this choice lies on the concept that goods and services are only worth what people are willing to pay. Monitoring a product sold through unofficial channels could be helpful to the publishers in further pricing of their products. Deciding a price just by calculating the costs of development, manufacturing, production and promotion and figuring out what is the lowest possible price requirement needed to break even is mathematically right, but does not take in consideration what ending users think about that price. So that, a grey market can be easily used by companies to run out market research and price testing in order to determine its most ideal/profitable price point. After the official launch, companies can fine tune their prices by comparing the data collected in every “place” their products are being sold, both for physical and digital copies. Also, the possibility to study the sales in an anonymous way can be useful to understand how consumers actually behave, without influence.

The second source from where grey market copies come are cheaper national or regional markets. Indeed, as for any other good sold worldwide, game prices differ depending on the country they are sold. That means that, in a different country, the same game would not necessarily cost the equivalent value given by the current monetary exchange rate. Taking advantage from localized pricing, lot of people use to buy a key from a cheaper region – like Asia – and then sell it in a more expensive one – like the US – at a higher price (but still lower than the official retailer) in order to make a profit.

In the last years, publishers started facing this phenomenon, creating limitations in the activation system. For instance, a Russian key cannot be activated on a US or European account. For that reason, grey market key sites started to label their keys if they’re region coded, to keep people from buying codes that won’t work due to the place they live. By the way, it is possible for people in lower economic regions like Russia to buy “Global” keys at a cheap rate and sell them on the grey market. In any case, codes are being bought and resold legally.

Even though people make profit selling a product without being a licensed retailer, is important to underline that this does not hurt publishers. Indeed, the company will make profit on each code through a price point they have approved before, on the official retail channels where the code was originally purchased.
Publishers could instead complain about potential lost revenues, coming from the price difference between the “secondhand” copy and the expensive region copy. In this case, it is not possible to prove that someone who bought a code for a grey market price would have bought that same item at the official price if the cheaper option was not available.

In the end, the developer is getting paid, and only one user is getting the game, because keys can be redeemed just once.

The same logic is applied to those who buy game codes at a profitable price because of a special deal period. Indeed, as well as traditional stores, online retailer put discounts on their products during shopping periods like Christmas and Easter holidays or the Black Friday. Some people may decide to buy codes at a deal price, and then sell them back on grey markets when the sale is over. This follows the simple “buy low, sell high” rule and, once again, the keys were obtained legally.

Some keys sold on grey market stores have been tracked down, and they found out that some of the codes were originally sent to journalists or reviewers as a “press copy”. Videogames users community pays close attention to YouTube or Twitch popular gamers, and publishers often give them free copies of their latest products in order to promote them.

Surely, selling a free copy on the grey market can be judged as unethical and unprofessional, but it is still a legal practice. Publishers could complain about the illegitimate sale of the key, because this was not the intended use, even though they did not paid for the keys in the first place, they are not exactly stolen goods either. Indeed, any gift legally belongs to the person who receives it, and he can arrange it as he wishes.

The question about grey market keys becomes controversial when they come from fraudulent or illegitimate purchases. Indeed, some individuals can legally buy game keys from official retailers using stolen digital payment credentials and then sell them at a lower price on unofficial platforms.

In 2015, Ubisoft deactivated hundreds of copies of their latest and more popular games, claiming that they were illegitimately purchased with stolen credit cards.³⁴ Here, the crime is upstream, and selling secondhand codes is just a way to “recycle” the money illegitimately spent.

This phenomenon is, by definition, included in the so-called *e-Fencing* practices: *in the world of criminal investigation, a "fence" is both "a receiver of stolen goods" and "a place where stolen goods are bought."

*The act of e-Fencing is the same exact offense, only it's done over the Internet, typically on online auction sites or classifieds like eBay.*

It is impossible or impractical for grey markets to check where each and every item comes from. For this reason, sites like G2A, Instant Gaming and Kinguin offer money-back warranties/guarantees on purchases made on their platform. In some cases, with an extra price the customer can get a sort of insurance, and in case the game is revoked the seller will either provide a full refund or another working code.

To sum up, we have seen that grey market stores are not properly part of piracy. They do not intentionally sell stolen or counterfeited keys, but this can happen as it is a hazard of a secondhand retail business.

**Deep Web and the Black Market**

After the analysis of the grey market, it is important to dedicate a short paragraph to the *black* market. Since we are talking about digital platforms dealing with digital copies, we must refer to the black market counterparts located in the so-called *Deep Web*.

Before reflecting on that, it is good to provide a couple of definitions.

First, the differences between what a grey and a black market are. While grey market deals with genuine goods that are sold outside the authorized channels, black market usually deals with banned, stolen or counterfeited. More specifically, black market is identified in the trade in items and services that are considered illegal by laws in the country or the region where the deal takes place.

Oxford Dictionary defines the Deep Web as *the part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks.* As many other technologies, Deep Web is not inherently “good” or “bad”, because this depends on the use that people do of it. However, its characteristics of anonymous contents and the

---

difficult (if not impossible) traceability of authors make it a perfect place for illegal purposes.

Leaving aside the ethical questions about the Deep Web, we must focus on the online anonymous marketplace ecosystem that it represents.

Indeed, that network hosts several online platforms, where any user can find almost everything. Taking in mind the black market definition is important to underline that most of the items sold on Deep Web marketplaces are illegal in almost every Country. Indeed, several surveys made on the most popular e-commerce platforms of the hidden network demonstrated that about 70% of the items available for purchase are drugs or drug-related products, followed by weapons and ammunitions of any kind, fake IDs and passports, stolen credit cards, confidential documents and illegal multimedia files. A very short percentage of items are actually legal or non-illegal, like the game keys or accounts that we can find on the grey market, as analyzed in the previous paragraph.

The reason of this lack of game keys on the Deep Web is easy to understand. People who buy the above-mentioned illegal items are potentially criminals, or at least they know well they are dealing illegal products with criminals. Who buys a weapon or a fake passport is aware of the fact he is violating the law and what could be the consequences of the committed crimes.

An individual that wants to purchase a videogame is not breaking any rule or law, even though he is looking for a discount. For this reason, he could be worried about being tracked down by the police and linked to criminals or criminal organizations. In other words, who decides to buy a videogame is not prone to take such a risk, because the economic value of this cannot be more than $20 or $30 – the average money they could save respect to the original product.

People who regularly or occasionally buy on the black market online stores and people who buy videogames belong to two different categories of consumers – even though some individuals can be classified in the two groups at the same time – and this allows us to exclude the Deep Web from the videogame piracy market.
CHAPTER IV
Conclusions

Through the analysis of the phenomenon of piracy and counterfeiting of digital goods, we have seen that its influence on the market and on the industry is lower than expected. Indeed, despite the constant threat of counterfeited copies spread in the market, videogame industry has been able to contrast the diffusion of piracy through technological development. Even though piracy always founded a way to break the protection measures adopted through the years, the main companies could protect their intellectual property and launch more advanced and performing products on the market at the same time.

However, the rate at which technology could help the companies to contrast piracy has decreased in the last years. When software solutions started to be less effective than before – or effective for a shorter time after the official launch of the product – Internet-based products gave a crackdown to industries dealing with Intellectual Property. The creation of brand new business models and new “products environments” has been a way to reconcile an excellent customer experience with a strong IP protection.

In the previous chapters, we have seen both theoretically and practically that piracy does influence video games industry less than expected, as well for any other digital product market. Recently, the European Commission has stated that there is no statistical evidence that illegal downloads affect legal sales for video games or other digital entertainment products.

In 2015, Dutch research company Ecorys has been charged with carrying out a research on the illicit consumption of films, movies, videogames, music and e-books across six European countries: Germany, France, United Kingdom, Spain, Sweden and Poland.

---

The report figured out that, during the previous year, an average of 51% of all adults and 72% of all minors in Europe illegally downloaded or streamed forms of digital entertainment.

With specific attention to the video games piracy section of the report, it is useful to look at the following table, which shows only 18% of respondents admitted to illegally streaming or downloading games, while only 16% admitted to playing on a chipped console:

![Table showing percentage of gamers in total number of respondents, by channel.](image)

**Figure 7: Percentage of gamers in total number of respondents, by channel.**

However, while the results highlight the presence of piracy within the European digital goods market, the European Commission does not merely accept the notion that this behavior can deter consumers from the legal purchase of the counterfeited and pirated copies of the same products. Indeed: "In general, the results do not show robust statistical evidence of displacement of sales by online copyright infringements," – the authors stated – "that does not necessarily mean that piracy has no effect but only that the statistical analysis does not prove with sufficient reliability that there is an effect."39

Among the results, indeed, the only warning data are related to illegal film consumption, with a 40% displacement rate for the latest releases, a percentage that hurts so much its own market. Furthermore, the report figured out that price cutting has any remarkable effect on consumers’ piracy propensity.

---

Concerning video games consumers' willingness to pay, it has been found that prices "are at a level broadly corresponding"\textsuperscript{40} to what those who illegally downloaded copy of a specific game would have paid for it.

Indeed, almost half of the people (55% of the sample) were willing to pay the market price or higher for their most recently illegal online transaction.

For this reason, the report claims that lowering the price of these products "would not change piracy rates".

The same results have been obtained on music and books samples, while the only market that would be positively affected by price lowering is the film one.

This partially confirms the hypothesis that people who download illegally and people who purchase legal copies belong to two different groups of people. In fact, the report added: "For books, music and games, the price setting alone cannot explain piracy levels because most pirates of those content are willing to pay more than extremely low prices."

On the other hand, is it also confirmed the hypothesis that piracy could have a positive effect on legal purchases, since people who download a counterfeited copy could enjoy the product and decide to buy a legal copy of it. This is highlighted by a 24% increase in the video games displacement rate, as shown in the table below:

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
 & Music & Films/TV-series & Books & Games \\
\hline
Displacement rate (coefficient) & + 0% & - 27 % & -38% & +24% \\
\hline
Nr. respondents & 13,896 & 15,851 & 11,383 & 11,226 \\
\hline
\end{tabular}
\caption{Estimate of displacement rates. Source: Estimating displacement rates of copyrighted content in the EU, p. 14.}
\end{table}

\textsuperscript{40} VV.AA., Estimating displacement rates of copyrighted content in the EU, p. 8.
The authors commented on such positive result as follows: "This positive effect of illegal downloads and streams on the sales of games may be explained by the industry being successful in converting illegal users to paying users. Tactics used by the industry include, for example, offering gameplay with extra bonuses or extra levels if consumers pay." 41

The results highlighted in this report are useful to confirm the reflections made during and after the previous chapters. Through the years, the industry focused fighting the piracy threat, claiming big damages to the business due to counterfeiting and violation of property rights. However, the continuous alternation of counterfeiting and new antipiracy measures has led to a sort of equilibrium between the legal and illegal consumption of digital goods.

We have seen how, at different levels, people who purchase legal copies through the authorized channels and people who always or often downloads counterfeited copies usually belong to two separated groups of consumers.

We can analyze this phenomenon as the natural evolution of the exponential transformation of the video games industry, which involved directly lot of actors from different categories, like companies, pirates, consumers and developers, and characterized by a high level of technology.

The theoretical framework highlighted in this essay could be applied to other companies or industries dealing with digital goods or products with a high technical evolution potential. The sensemaking strategies useful for this purpose are essentially two: the narrative one and the quantification one.

Indeed, while a narrative description of a case can highlight the similar evolution between an environment with an increasing counterfeiting threat and the environment described in the previous chapters, a quantitative analysis can give statistical meanings to raw data, in order to confirm that theory.

---

41 VV.AA., *Estimating displacement rates of copyrighted content in the EU*, p. 15.
References


Cox, C. (2012, August 22). *Ubisoft: 'Vast majority of PC gamers are PIRATES'*. Retrieved from The Register: www.theregister.co.uk/2012/08/22/ubisoft_says_over_90_per_cent_of_pc_gamers_are_pirates/, visited on January


Martin, J. (2008, February 15). *Nintendo lost $975 million to piracy last year.* Retrieved from Bit-Tech: https://www.bit-tech.net/news/gaming/nintendo_lost_975_million_to_piracy_last_year/1/


# Table of Figures

Figure 1: Total games available on Steam. Source: Steamspy (www.steamspy.com) ................................................. 9

Figure 2: World Game Console Market by Platform and by Company. Source: HIS Markit ........................................ 10

Figure 3: World Digital Games Console Market by Company (2015-2017). Source: HIS Markit .............................. 12

Figure 4: Global Games Market in 2017. Source: Newzoo ..................................................................................... 13

Figure 5: Bill Gates' open letter to computer hobbyists. February 3, 1976. ............................................................. 18

Figure 6: Dynamics of sales and downloads for a popular album. Period expressed by week, sales and downloads in thousands. ......................................................................................................................... 37

Figure 7: Percentage of gamers in total number of respondents, by channel ........................................................... 68

Figure 8: Estimate of displacement rates. Source: Estimating displacement rates of copyrighted content in the EU, p. 14 ....................................................................................................................................................... 69