

```

C:\Users\User\Downloads> cd /
Volume in drive C: is OS
Volume Serial number is 0133-7058K

Directory of C:\Users\User\Downloads

[.]
[..]
[Appz]
[Gamez]
[Muzic]
[Moviez]
[TV]
[WINDOWS 7-ULTIMATE-32 BIT+WAT REMOVER - ZIP]
Adele - Rolling In the Deep [2010-Single][SW].zip
Adobe.Creative.Suite.5.5.Design.Premium.Retail.ISO-CORE.iso
All New Electronics Self-Teaching Guide 3 Ed - (Malestrom).pdf
Black Eyed Peas - Just Can't Get Enough [2011-Single][SW].rar
Black Eyed Peas - The Beginning (Deluxe Edition) 2010-DOWN.zip
Call.of.Duty.Black.Ops-SKIDROW-[tracker.BTARENA.org].iso
Dr. Dre - I Need a Doctor (feat. Eminem) [2011-Single][MJN].rar
GTA San Andreas full game pc <<with crack>>.iso
Hacking - Firewalls And Networks How To Hack.pdf
Half-Life, Half-Life 2 [+ Episodes], Portal, and The Orange Box.rar
How to Blow Her Mind in Bed: The essential guide for any man.pdf
I ROBOT 2004 * 720p BRRip * x264 AAC * M777 M2Tv.mkv
Lady Gaga-Born This Way (Special Edition) 2CD 2011-pLAN9.rar
Me, Myself & Irene (2000) 720p BRRip x264-iND3X.mkv
MICROSOFT OFFICE 2010 PERMANENT ACTIVATOR [thethingy].zip
Microsoft Office 2010,Pro.Plus,X64+X86+Reg.by ErikB.NL.iso
Minecraft Beta 1.1_02 (Updatable) [Fullversion] [EN] - iHack4Yo.iso
Mirrors.Edge-(OST)-2008-OSTKingZ [Mitzrokk.Stereo.Reseed].zip
Need.for.Speed.Hot.Pursuit-RELOADED.iso
Nero 10.0 + Serials - DivXNL-Team.rar
Pink (Pink) - Raise Your Glass [2010-Single][MJN].rar
Snoop Dogg - Sweat (David Guetta Remix) [2011-Single][SW].zip
The Five Secrets You Must Discover Before You Die.pdf
The Hangover (2009) UNRATED BRRip 720p x264 AAC-Ameet6233.mkv
The Sims 3 Generations-RELOADED.iso
Transformers.Duology.BluRay.720p.DTS.x264-HDLiTE.mkv
WinZip PRO FINAL v15.0 + Serials [ChattChitto RG].zip

27 File(s)          356,365,139 bytes
 6 Dir(s)           11,987,742,720 bytes free

```

## PIRACY IN THE DIGITAL AGE

An essay about piracy in the digital age. Is it really that bad?

BY: James Ingles



Piracy in the digital age – An essay about piracy in the digital age. Is it really that bad? By James Ingles is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

Based on a work at [kulture.com.au](http://kulture.com.au).

You are free to :

**Share** — to copy, distribute and transmit the work

**Remix** — to adapt the work

Under the following conditions:

**Attribution** — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

**Attribution specification:** If you alter, transform, or build upon this work then I would request that you link to <http://www.kulture.com.au/piracy/> and that you send me a link to your work based upon this essay. I would like to see where this goes.

**Noncommercial** — You may not use this work for commercial purposes unless I the author, James Ingles, gives permission.

**Share Alike** — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

With the understanding that:

**Waiver** — Any of the above conditions can be waived if you get permission from the copyright holder.

**Public Domain** — Where the work or any of its elements is in the public domain under applicable law, that status is in no way affected by the license.

**Other Rights** — In no way are any of the following rights affected by the license:

Your fair dealing or fair use rights, or other applicable copyright exceptions and limitations;

The author's moral rights;

Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.

If you wish to use this work in a way that is not allowed by the licence please contact me by leaving a comment at:

<http://www.kulture.com.au/piracy/>

# What is piracy/copyright infringement?

Piracy/copyright infringement is the act of obtaining and using a copyrighted work illegally whether it is a book the use of a copyrighted song, watching downloaded movies, playing of a game or use of an application that was not obtained legally i.e. using something that was not paid for or using a copyrighted work in a way that you do not have the rights to use.

For example: someone makes a home movie and uses a copyrighted song in the said home movie they are breaking copyright because they do not have the right to use that audio track in a movie. Whether or not they illegally downloaded the song from the internet or whether they ripped it from a CD they paid for, the law still says that use is illegal however they obtained the piece of music. The latter use I would argue is not at all wrong because they are probably not making money from their home movie. But that is a whole other can of worms that I'm not going to open. There are plenty of ways that copyright can be infringed. I'm going to look mainly at computer/internet piracy and how people infringe copyright by obtaining copyrighted materials and not how those copyrighted materials are used, do you really need to have it explained to you how someone uses a movie that they illegally download? Really? Seriously? Well they probably just watch it. But I digress.

For the sake of this essay piracy and copyright infringement are the same thing. I will use the word piracy and copyright infringement to mean the same thing, I will use the two terms interchangeably, that is the acquisition and unauthorised use of a copyrighted work whether it be a game, application, movie, DVD etc...

I became interested in the issues surrounding internet piracy when I discovered free and free open source software after I had to fix my PC after my web browser got hijacked due to my somewhat dodgy surfing habits related to piracy. Prior to that nearly every piece of software that I used on my PC was pirated from the pirated copy of Windows XP, Microsoft Office, to Nero for burning CDs and ACDSee for viewing photos. I would regularly get infected with viruses and have to fix my computer, which is part of the reason of how I came to learn so much about computers i.e. how I became a geek, I'd break it then I'd fix it. Ultimately I discovered that free and free open source software can be as good if not better than software that you pay for, it can also be worse but rarely is that the case. It has been a bit of a journey for me and with all the hype surrounding piracy I figured it was high time that piracy and all the issues surrounding piracy be looked at in some depth. So I decided to write about it, this essay is part story of my own personal journey, part fact, and partly my own thoughts on the subject. A lot of the information contained within is gained from personal experience, some is personal opinion, educated guesses based on personal experience and information found on the internet, the rest is gathered from articles and studies about piracy and research that I have found on the internet.

Piracy isn't only an issue for software, game, movie & TV producers, and the music industry. The entertainment industry just make the most noise about piracy, piracy also affects book publishers, video/image producers or anyone that produces content that is or can be digitised. When I talk about piracy I mean any sort of piracy, piracy in general. I will use figures about tv/movie, music, application, and games piracy because they are more readily available because they are studied more and because those industries make the most noise about piracy.

I'm not going to say piracy is bad and you are going to go to hell or get sued to bankruptcy by the RIAA, MPAA, BSA or any other group that is vehemently against piracy. Nor am I going to say piracy is a good thing either and that you should pirate, I will try to remain neutral. I am not going to throw stones because I am not without sin. I don't propose to have all the answers about how to stop piracy, not that I think it should or ever will be stopped. Piracy is here to stay. What I do think is that piracy has its place in the digital ecosystem and that is what I want to do with this essay; take a comprehensive look at piracy and its place in the digital ecosystem, in this the digital age.

## My own journey

Unlike some kids who don't know life without computers, like my younger cousins, I haven't always grown up with computers I remember life BC, Before Computers. When I say BC I mean a time when computers were generally large, costly systems owned by large institutions, corporations, universities, government agencies, and the like. A time when PCs were not as ubiquitous or as user friendly as they are today. Computers were

still around and we did use them but not in the way we use them today. They were almost invisible. I wonder how many people knew that ATMs were powered by computers, or that in the early 90s the internet, email and the WWW were just being born? Computers have been around for a long time but they weren't always personal.

In the time before computers I used to dig great big holes that were nearly as deep as I was tall in the back yard, then I'd fill them with water and jump into them. Or I'd ride my bike, draw, or play with my Lego. Lego used to be my crack, I played with it for hours and hours every day, I had heaps of it and would build entire cities out of Lego. Later on I got into Lego Technics and collected quite a few models, with pneumatics and motors. Then one day I lost interest when friends of my parents brought their ungodly abomination of a child along who delighted in wrecking my city of Lego that took me weeks and weeks to build and perfect. Once the little bastard child destroyed that it moved on to disassembling my Lego Technics models in the most violent way imaginable. That destroyed me inside, I kind of lost interest in Lego after that terribly unfortunate incident. Luckily karma is real and I know that she is a real bitch, I just wish I could see that horrid creature get it dues. But I digress. After that I moved on to collecting stamps and coins after my father bequeathed his stamp and coin collection on me and I gained a new interest. I collected stamps and coins for a few years and I really enjoyed it. None of these hobbies really had anything to do with computers. For a long time I never knew about computers or even really cared for them. It wasn't until I got interested in electronics that I started to get interested in computers. I would find all sorts of dead, sometimes living electronic equipment, and started dismembering some poor unsuspecting TVs, radios, anything with a PCB, resistors, IC's, ect... Even my old Commodore 64 didn't escape the fate of death by screwdriver. Boy do I regret pulling that apart! I still regret sacrificing the Commodore 64 to this day I, obviously I didn't care for computers at that stage in my life, there was still hope for me, given that I was willing to disembowel a living Commodore 64 just to see what was inside and how it worked. If I knew what an important bit of hardware it would have become, and how much I could have sold it for I would never have attacked it with the screwdriver. I never did figure out how the contraptions worked, I just enjoyed seeing all the parts that made it work. I thought it looked cool, I was just a bored kid who amused himself by taking a screwdriver to any electronic equipment I could get my hands on. Seldom did anything get fixed or even put back together, which was usually because I had destroyed it to get it apart in the first place. To me a computer was just something to play video games on. I didn't have a grasp on how influential computers were or would become. To me computers were just another bit of electronic equipment. I didn't have any idea on how beneficial computers would become in everyday life nor did I have any inkling that computer skills would benefit me as much as they have.

It was an uncle that fuelled my interest in computers by showing and explaining when ever I'd ask about something to do with the computer. My uncle was an uber computer geek. Being disabled and wheelchair bound for a big chunk of his life courtesy of a car crash at a young age, it certainly wasn't part of his plan for life. He certainly wasn't going to run in the Olympics or become the next 10 pin bowling champion. So he found another hobby that didn't require walking or the use of legs in any way, a hobby that you could sit down and be good at, in any kind of chair with wheels or sans wheels. That hobby was computers. All that time spent with computers paid off. The skills he developed became really useful and rubbed off on me.

I was still in primary school when I started to get into computers. I was amazed at what they could do and have been addicted ever since. For most of my life I have grown up with and around computers, our family has had a computer and I have had my own computer for most of my life too.

Our first computer was a Commodore 64 that came with a bunch of pirated games. At the time I was too young to know, or even care that the games were pirated. I remember having to get dad to lug in their big old CRT TV (it was the 90s) and hook it up to the computer so we could play the games that came on 5 1/4" floppy disks. Our favourite game was Boulder Dash 2. We played it for hours on end together. We would flip a coin to see who would go first. When they died it was the other persons turn to see how far they could get. It was great fun, now the extent of my dads gaming experience is made up entirely of solitaire on the old 5 year old XP machine. Even my mum found Burger Time and got into gaming for a little while, years later I found a remake of burger time that I downloaded for her that she played a little bit. Now my Mum prefers to play those brain training games (and takes great delight when the contraption tell her that her brain is a lot younger than she actually is) on her Nintendo DS that I gave to her after I grew bored of it. My sister never got into computers or games until the Wii came out, but now I think she is bored of it and barely plays the Wii.

Our first modern PC was a 386 SX which ran at 66 Mhz, had 4 MB of ram, a 220 MB HDD and ran Windows 3.11. By this time I was addicted to computers like a fly is to shit. We had to draw up a computer roster otherwise fights would break out between my sister and I about who's turn it was and how long the other person had been on the computer for. It was during this time that I started to want my own computer. I'd read computer magazines and look at computers way more than was normal for most kids my age. it wouldn't be

long until I got my own computer.

I got my very own computer as compensation for not being able to go to the US on a school exchange trip that I had applied and been accepted for. My parents were awesome enough to get me a computer of my own. It was a 486 DX that ran at 100 MHz, had 16 MB of RAM and an 850 MB HDD at the time it was an awesome PC. Around the same time we got an internet connection, something else for us to fight over. We had a 56.6 Kbps modem, the fastest internet connection the public could get at the time.

Not long after we got our first internet connection I discovered MP3s, which were still unknown to the common noob who still brought CDs. I had discovered MP3s and where I could get them for free, free music! Awesome! Yeah I'm a geek who was into MP3s before before they were cool, before Apple iTunes. MP3s were great I could have music on my computer and I could convert my CD collection to MP3 as well, awesome! Over time my MP3 collection grew so big that most of my 850 MB (and later on 2.6 GB HDD) were filled with MP3s. So I got a 2x CD burner for my birthday and started burning CDs. I accrued thousands of MP3s on nearly 100 CDs over a few years with a dialup internet connection.

I was still too young to have a job to save up and upgrade my PC, but I did get pocket money \$10 a week. It was going to take me for ever to save up for a better PC at \$10 a week. I didn't even know you could build your own PC at the time. I knew they could be upgraded but I didn't know how, but I did have an uncle that did know who taught me quite a bit about computers over the years. So I saved my pocket money and convinced my parents to help fund an upgrade if I chipped in with my pocket money. For my birthday that year I got an upgrade. I upgraded to a Cyrix 686 PR200+, 32 MB of RAM and a 2.6 GB HDD. I got a copy of Windows 95 and Adobe Photoshop 4 and a bunch of other programs. My uncle would burn me CDs full of games and applications. This is when I discovered warez. The penny had dropped that I could download games and applications for free. I discovered places where I could get pretty much anything I wanted from IRC warez channels, I learned about cracks, patches, serial generators (which usually come laden with all sorts of nasty malware), FTP sites and later on BitTorrent. I was young and didn't know or really care that it was illegal since either being given or downloading software was to my mind acceptable and the normal way to get games, applications and music.

Things happened and I lost my uncle who would upgrade my computer, who would teach me about computers. If something broke I was on my own, by now I knew enough to be able to teach myself with the aid of the internet. When I got my first virus I had to reformat my PC, I took what I had learned from my uncle and hit the internet. I had started reading and learning more about computers. I learned how to fix my computer so when I got viruses from using illegal software (usually from the cracks, patches and key generators that I would download) I didn't really care. I'd just fix it. And fix it I did, plenty of times. I was becoming a pro at reformatting and installing illegal copies of Windows 95/98/2000 and XP. I was getting sick of just playing with software and started wanting to build my own computer.

For years I had wanted to build my own computer but could never afford the hardware. Now that I was old enough I went and got myself a part time job while I attended TAFE so that I could build on skills that I had learned thanks to the wonders of warez and the internet. My first job was at Hungry Jacks (something I am not proud of, but I guess it's not the worst job I could have been doing and it was certainly better than a kick in the pants) I started saving money. I left Hungry Jacks, well got fired because I'd rather hang out with my girlfriend at the time, so I got a new job. My new job was a web site administrator, for a small business that had the worst web site that I have ever seen, even to this day I have not seen a worse web site. It was truly the worst web site in the history of the internet, but I guess someone has to have a the worst web site. I got this job with skills that I had learned from the internet and skills I had taught/developed myself with illegal software that I had downloaded and used, Dreamweaver (back when it was owned by Macromedia, before Adobe brought them out), Photoshop, Illustrator, CuteFTP and a bunch of other programs. By this time I had had enough experience from upgrading my old PCs to not only build the PC I wanted but install and configure the operating system. While I worked that job I saved more money and built myself my own PC. I had wanted it so bad and I could finally build the PC that I wanted not some PC that someone else told me I wanted. I was not going to be advertising's bitch and buy the PC that I was told to buy. I spent over \$5,000 on the new PC then pirated a copy of Windows XP Professional which was the latest and greatest Microsoft OS at the time. I had that PC for 5 years, in that time I learned a lot more about computers simply because I had to, because I didn't have anyone else to teach me and it was expensive to have a computer technician fix my PC. It was out of necessity that I learned how to build, troubleshoot and fix PCs.

Around the same time that I built my own PC that I also migrated from dialup internet access to ADSL which had become more common and affordable. I had a job and could afford to contribute to our communications cost. I was still living at home so I educated my parents (as well as myself before I sold it to my parents) about ADSL so they would let me install it on their phone line, the biggest selling points were that we would

save on the cost of a local call to dial an internet connection, it wouldn't tie up the phone line and more than one person could be on the internet at any one time. Finally the fight for the dialup modem was dead. ADSL was great I learned some new skills (thanks to the warez, or more accurately, my wanting of warez) and I could download a lot more a lot faster! The first ADSL connection we had ran at 512 Kbps and I thought it was great, then I upgraded to a 1.5 Mbps connection, even better! Triple the speed of our first connection! I could do so much more and a lot faster too. Then I upgraded to ADSL 2+ which I am on right now.

By the time I built my second PC 5 years later I had grown up and had all but stopped downloading warez because I was getting sick of getting viruses from illegal software and wanted to keep my PC malware free. I even paid for a copy of Windows Vista (twice, because later on I built a HTPC so I brought another copy of Vista), then when Windows 7 came out I brought a copy and upgraded my gaming rig. There is one event that sticks out in my mind that lead me to reduce my piracy more than anything else.

For a long time I had known that there was free software out there that didn't contain viruses like some illegal software does but I never used it because I was naive enough to think, like a lot of other people, that free software wasn't going to be half as good as software that you had to pay for. There are a lot of common misconceptions about free and FOS software, like it's not as secure, it's not as good and doesn't have features that people need. I kept pirating software and getting viruses and contracting all sorts of exotic malware infections.

There was one event that made me take a good hard look at alternatives, and change my ways. It was when I was still using Windows XP professional that I had illegitimately downloaded and installed and I still used Microsofts (don't laugh) Internet Explorer web browser. IE started taking me, forcefully, and against my will, to web sites that were pushing all sorts of rubbish, like programs that would fix the problem I was having. I was smart enough to know that the programs being pushed were total BS and were full of even more malware that would let scum bags access my PC remotely so they could mine my PC for financial data and other information that could be used to steal my identity. So I hoped on our other computer and researched my problem. I found a out that my browser had been hijacked, which wasn't surprising given all the dodgy web sites that I'd used to visit in my quest for free but illegal software. I discovered how to reclaim my browser. I fixed the problem although it took hours to resolve and I was considering even just reformatting the PC but that was a last resort that I thankfully didn't have to resort to. During the incident (which was directly related to downloading warez and illegal software) I learned a lot about computer security and that IE, the default browser that comes with Windows, is terribly insecure. The second I claimed my browser back I downloaded and installed another web browser which was free, it was called Opera which I loved and still use. Opera was still, ignoring the point releases, in single digit version numbers (I started using Opera around version 5 or 6 or possibly 4, it was such a long time ago I don't exactly remember) at the time but it was a lot faster than IE on my aging machine, it made my machine feel faster. Web pages loaded so much more faster and it had a lot of features that were actually useful that made browsing a lot quicker and easier like mouse gestures. The biggest surprise was that it was free and it was better than IE which you essentially paid for anyway because when you buy (not that I paid for my copy of Windows) a copy of Windows which install's IE when you installed Windows. The other revelation was that the software tools that I used to fix my problem were also free. This was enough to make me start looking at free alternatives to programs that I had been using illegally or that I have been paying for. I changed to a free antivirus program (the AV program that I used to use I had to pay an annual subscription to) and started using other free antimalware tools to keep my system clean. I had learned that free software can be just as good and better than software that you have to pay for.

Although I still pirated games but not as much as I used to. I had always paid for a lot of games that I liked and played but I had also pirated a lot of games. The games I paid for were games that I really wanted and enjoyed, like Heroes of Might and Magic, Crusader: No Remorse, Crusader: No Regret, Half Life 2, I played those games all the way through and replayed them more than once. The games that I pirated were usually half played then deleted them or are lost in my terabytes of data that I had collected over the years, data that I can't be bothered going through. The pirated games were so rubbish I was never going to pay for them anyway. Then on 22 March 2002 Valve released Steam which would revolutionise the gaming industry. Steam also got me to pay for games. I was a bit late jumping onto steam but I have since warmed to Steam I have purchased a bunch of games, a bunch equals 48 and counting. Some of those games I brought because they appealed to me at the time and they were cheap so I brought it then never played it or only half played through the game before I got bored. I don't mind that I have paid for games I haven't played because I know I can download and play them any time. That and the games were so ridiculously cheap it doesn't matter and I know I'm downloading a legitimate game and not playing Russian roulette with viruses, I know the Steam game is virus free so I can install it and not have to wonder if it's infected with viruses or not and I don't have to feel guilty. I have even started buying music legitimately and have brought albums that I had downloaded illegally even though I already had those albums.

Now I have discovered free alternatives for a lot of programs that I had been pirating in the past. Even better a lot of the software was Free Open Source Software (not to be confused with Open Source Software which you still have to pay for) which makes me warm and fuzzy inside. Now 80% of the programs I run are free or FOSS, and the rest are either OEM copies of software that I got with hardware and the only software I have paid for recently, apart from Games from Steam, are my copies of Windows Vista and Windows 7 operating systems that I have used in my last 2 PC builds. I'd use Linux but I like to play my AAA title games without having to fart arse about in the hope of getting them to work, but that's a whole other can of worms. My aim was to stop viruses taking over my computer and rendering it so far beyond repair that I have to reformat my PC. I can say that I achieved that result because since the browser hijacking incident I started taking my own computer security a lot more seriously and I can't remember the last time I contracted a virus or any malware that forced me to have to reformat my computer or waste hours fixing/removing. Now as a computer technician it frustrates me how many computers I see come through the workshop with viruses, and I know exactly how they go the viruses; piracy.

## A history of piracy

For as long as computers have been around so to has piracy but the history of piracy goes far back beyond the invention of the computer and back to the 1500s when Gutenberg invented the printing press.

Before the arrival of the printing press in Europe in the 1500's information was highly scarce and relatively easy to control. For thousands of years, the scribal culture hand-picked the people who were given this code to transmit knowledge across time and space. Knowledge was an economy of scarcity. The arrival of the printing press would change how knowledge is distributed. Print brought with it a new abundance of information threatening the control over ideas and knowledge that had come with scarcity.

Books were about to change everything. Books weren't always as readily available as they are today. Books were a new communications technology that was seen, by the church, as the unholy work of the Devil. Daniel Defoe tells of Gutenberg's partner Johann Fust, arriving in 15th century Paris with a wagon load of printed bibles. When the bibles were examined, and the exact similarity of each book was discovered, the Parisians set upon Fust accusing him of black magic.

So dangerous was this knowledge that books were kept under lock and guard. There are images from the 16th century of books that were chained to big heavy immovable objects, and had to be guarded by armed guards outside a heavy door because it was very, very dangerous for people to have access to the knowledge contained within. People were in a sense starved for knowledge.

All of the emerging nation-states of Europe made it very clear that they would control information flows to the best of their ability. The printers were the ones who were hunted down if they printed the forbidden text rather than the authors it was really the printers who suffered most.

As print technology developed in Europe and America its pivotal social role became clear. Printing became associated with rebellion and emancipation. The governor of Virginia, Governor Berkeley wrote to his overseers in England in the 17th century saying, "Thank God we have no printing in Virginia," "and we shall never have it as long as I'm governor." This was a reaction to the English civil war and the pamphlet wars, pamphlets were called paper bullets in that period.

The basic idea of censorship in 18th century France is a concept of privilege, or private law. A publisher gets the right to publish a particular text, that is deny it to others, so he has that privilege. What you have is a centralised administration for controlling the book trade, using censorship and also using the monopoly of the established publishers. They made sure that the books that flowed throughout a society were authorised - were the authorised editions - but also were within the control of the state within the control of the king or the prince. You had a very elaborate system of censorship but in addition to that you had a monopoly of production in the booksellers' guild in Paris. It had police powers. And then the police itself had specialised powers as well, they were inspectors of the book trade.

If you put all of that together you see that the state was very powerful, but its attempt to control the printed word ultimately failed. But not only was it's apparatus incapable of preventing the spread of revolutionary thought, it's very existence inspired the creation of new, parallel pirate systems of distribution.

What is clear is that during the 18th century the printed word is expanding everywhere. You've got publishing houses printing presses that surround France with dozens and dozens of them producing books which are smuggled across the French borders distributed everywhere in the kingdom by an underground system.

One Dutch printer looked at the index of prohibited books and used it for his publication program because he knew these were titles that would sell well. The pirates had agents in Paris and everywhere else who were sending them sheets of new books, which they thought would sell well. The pirates are essentially doing market research. They are sounding the market. They want to know what the demand is. The reaction on the part of the publishers at the centre is, of course, extremely hostile. In actual fact, many of these pirates were good bourgeois in Lausanne or Geneva or Amsterdam and they thought that they were just doing business. After all, there was no international copyright law and they were satisfying demand.

There were printers that were almost holes in the wall if they were printing subversive material they could hide their presses very quickly. People used to put them on rafts and float down to another town if they were in trouble with the authorities. It was very movable. In effect, you've got two systems at war with one another. It's this system of production outside of France that is crucial for the Enlightenment. Not only did this new media system spread the Enlightenment, but it so indicted the Old Regime that this power - public opinion became crucial in the collapse of the government in 1787-1788. In Paris, the Bastille had been a prison for pirates. But in the years before the Revolution the authorities gave up trying to imprison pirates. The flow of ideas and information was too strong to be stopped.

That's the dramatic change that was affected by the printing revolution, that all of a sudden the emergence of a new reading public the emergence of an undisciplined reading public which were not subject to the same norms of reading or the same norms of relation to knowledge as it was in the past. It was a dramatic shift. The fundamental urge to copy had nothing to do with technology. It's about how culture is created. But technology of course changes what we can copy how quickly we can copy and how we can share it.

## **Modern piracy - piracy in the digital age**

There have been many technological advancements that have aided piracy and copyright infringement. There are two main advancements in technology after Gutenbergs printing press, that have accelerated the rate of piracy more than anything else; computers and the internet. It's the digital revolution, the information age, the digital age or what ever you want to call it. It's here and it's not going away.

The development of floppy disks and more recently CDs/DVDs/Bluerays, USB thumb drives, memory cards, and portable hard drives made it cheap and easy to store and transport large amounts of data, legal or otherwise. On the software side we have the development of programs like FTP clients, web browsers, BitTorrent clients and other P2P programs which make piracy easier and more accessible. Although all the programs and large amounts of cheap storage would be next to useless without cheap high speed internet connections like ADSL or cable internet combined with large download limits that make it easier and faster to copy and move all of that illegal data about from one side of the world to the other or from one PC to another. The falling cost of computer hardware, the increasing speed of computers and the accessibility of PCs has also pushed piracy to the level that it is at today.

Computer components are always getting cheaper, faster and better, all the time. Processors or CPUs are getting faster, more and more RAM can be crammed onto a single DIMM, video cards are getting faster and better. The modern PC makes it possible to do things that could only be dreamt about when computers were first invented. Apart from running applications and playing games, PCs are now capable of playing back high definition movies, playing back CD quality music and a lot more. Although PCs are getting cheaper people are still spending a lot of money on hardware. After spending a bunch of money (the last 2 PCs I have built cost me over \$5,000 each) on awesome new hardware there is little to no money left to pay for the software and games to run on the machine, without software like the Operating System that new PC is just a giant, expensive, novelty paper weight. There is also no money left for going to the movies or buying CDs or DVDs to play on the new PC so people save money by pirating what they need (software like an Operating System, usually Windows) and want, games, movies, music, TV shows ect...

Before computers could play music or movies, shows and movies were taped from TV and copied from VHS tapes, cassette tapes were used to record music off the radio. Games, applications and other forms of piracy were a lot lower than they are today because computers still hadn't entered the mainstream, they were still in the realm of large corporations, universities and the hardcore hobbyist. Piracy was a lot more expensive and

labour intensive before computers as it required you to buy the hardware then you had to buy the blank media like VHS tapes or cassette tapes. If you wanted to copy a VHS tape you would need 2 VCRs, all the right cables as well as blank tapes and the know how. If you were copying a cassette tape you would need a dual tape player or two tape players as well as the cables and blank media.

Before computers became as common and accessible as they are now piracy was more expensive, time consuming since money was needed to buy the hardware and the blank media, you had to have the time and knowledge to do it or know someone with the money, hardware, time and knowledge to do it. Or know someone who could get their hands on pirated material. Piracy was less of a problem because of the higher cost and labour involved and it was only TV shows, movies, and records that were commonly pirated. The other problem with copying VHS and cassette tapes is that the quality would degrade with each copy so piracy wasn't a major issue.

Computers would change all of this accelerating piracy to the level that it is today by making piracy more accessible, easier, cheaper and faster. Computers also changed what could be copied and each copy would be a 1:1 copy without any of degradation that VHS and cassette tapes suffered from.

In the 80s PCs became popular (Apple II, Commodore 64, the Atari 400 and Atari 800, the ZX Spectrum, the Amiga, the Atari ST, and other PCs) and piracy became a bigger ongoing problem ever since high quality, commercially produced software was released for sale to more people than before. Games and applications started to be pirated as well as TV shows, movies, and records. Because computers weren't yet powerful enough to play video or music TV shows, movies, and records were still being pirated the old fashioned way with tape decks and cumbersome VCR set ups.

Back in 1980 the first 1 GB HDD (the IBM 3380) was the size of a refrigerator, weighed 550 pounds (about 250 kg) and cost \$40,000<sup>43</sup>, now a 1TB HDD has more than 1000x the capacity, weighs less than 0.5 kg, is around 4x5 inches and costs \$59. In 2010 it is hard to find any type of storage media that will hold 1 GB, even the smallest micro SD cards can hold 4 GB or more of data. Not everyone could afford a \$40,000 1GB HDD, floppy disks were a cheaper alternative and was the media of choice for a long while. If someone wanted to copy data they would just copy the floppy disk with a program like Locksmith that was intended to make "backup copies" of programs which, ironically, was widely pirated.

Most people didn't even have an internet connection at this stage, although the internet was alive and growing rapidly. Disks were mailed via the postage system, aka mail trading, if data needed to be copied over vast distances. Floppy disks and postage was cheap which made it a good method for piracy. However it still cost money.

The next big technological advancement was the internet, or more specifically the commercialisation of the internet which would, amongst other things, allow users to copy data between computers around the world quicker and easier than ever before.

At 22:30 hours on October 29, 1969 The first ARPANET link was established, ARPANET would later evolve into the internet as we know it today but it wouldn't be until the early 80's when the internet is commercialised, and the 90s when the first ISPs would be formed and the internet would really start to take off in popularity.

In the 60s, 70s & 80s there were many different types of computers, and there were no formal standardised as such, i.e. it wasn't as simple as Windows or Mac, or if you are really geeky Linux or Unix. Also internet connections weren't standard there were only a handful of different online service providers who had different systems which were all incompatible with each other, each service also had different features. The internet as we know it didn't really start taking shape until the mid to late 70's.

In 1975 Telnet went online along with Tymnet and is the first public information super highway. Later in 1978 Compucom, later to become The Source, goes online. Also in 1978 the first BBS goes online, BBS's would later grow in popularity. 1979 sees MicroNET (later CompuServe) and The Source open up to paying customers. The first Usenet news group goes online in 1979.

BBS's were developed by Ward Christensen and Randy Suess, according to an early interview, while they were snowed in during the Great Blizzard of 1978 in Chicago. Christensen along with fellow hobbyist Randy Suess, began preliminary work on the Computerized Bulletin Board System, or CBBS. On February 16, 1978 the CBBS went online in Chicago, Illinois<sup>45</sup>. BBSs were accessed by a modem connected to a phone line. Initially access was slow, with speeds of 110 and 300 bits per a second. In the 80s modem speeds increased to 1200 bits per a second then, 2400, 4800 and 9600 bps. In 1991 modem speeds were increased to 14.4 kilobits per second, in 1994, speeds doubled to 28.8 kilobits per second. Soon after, there came 33.6kbps,

which was thought to be an upper limit for phone line transmissions. Then in 1996 Dr. Brent Townshend developed the 56k modem<sup>44</sup>. Although access to BBSs was still expensive as the user was still paying for a timed call. If the BBS number was a long distance number then the charges would be higher than the charges for a local call.

It was in the 80s when PCs had become more popular, cheaper, faster, storage capacity had risen, and the internet had evolved a bit further. In 1982 the first alternative to ARPANET, CSNET, goes online as a low cost alternative to ARPANET for universities that don't qualify for ARPANET access. But it wasn't until the late 80's before the average person could get access to the internet. In 1989 the first public Internet Service Provider, The World, is opened by Software Tool & Die Company. A few months later Applelink – Personal Edition came online, but it didn't last long. Quantum opens PC-Link, a partnership with Tandy for IBM compatible computers. The Source gets brought by CumpuServe who pull the plug on The Source. In 1990 Quantum reopens it's Apple II service and re brands it as America Online, AOL. Prodigy is launched and declares itself the “first consumer online service” despite there being other online consumer services that came before it. Genie also launch Star Services another ISP. Many other ISPs popped up world wide offering internet access. In 1990 Tim Berners-Lee invents the Hypertext Markup Language that will become synonymous with the World Wide Web.

It was in the mid 90's that the World Wide Web (also commonly referred to as the information super highway at the time or sometimes just the web) as most people know it came into existence, thanks to Tim Berners-Lee, and became mainstream which resulted in a decline in popularity for BBSes, although some of the larger commercial BBSes, such as ExecPC BBS, became actual Internet Service Providers. The World Wide Web, or WWW, turned out to be the killer application for the internet that would drive people to get an internet connection. The uptake of internet connections sky rocketed in the 90's.

The web made it easy to share information. If you knew how to code HTML and had a web host you could create your own web page and share your knowledge about whatever topic you like. The beauty of the internet is that anyone can publish anything they like and it's not regulated. It didn't take long before people were sharing copyrighted material via the web and other internet protocols like FTP, IRC and Usenet. New programs would be written and new protocols would be developed to help share information. The web would be used to publish information on how to find and download anything you want, this sort of information would never have been published in the printed press. The web was a place that was free for all and has been referred to as the wild west because of it's lack of rules and formalities.

Before broadband users would connect to the internet via a dialup modem. The speed of a dialup modem ranged from 110 baud with a maximum speed of 0.1 kbit/s, through to the fastest dialup modem a 56k (V.92) that had a maximum speed of 56.0/48.0 kbit/s which in perfect conditions was capable of receiving data at 7Kb/s. There were technologies like hardware and Server-side compression that could increase throughput by compressing data, but the speed was still slow by today's standards. Dialup still suffered from some of the same problems that ADSL suffers from, I.e noisy phone lines which would mean that connection speeds were often slow. But there was a bigger problem with dialup, it could be terribly expensive. Each time you dialed a connection you would be paying for the cost of a phone call. And if you didn't pay a flat rate for phone calls, i.e. you payed per a minute then the longer you kept the connection open the larger your phone bill would be. If, back in the hey day of BBSes, the BBS you dialed up to was a long distance number then you could expect a large phone bill, likewise if your dialup ISP didn't have a local PoP (Point of Presence) then you would be paying long distance calls which aren't cheap.

With a dial-up connection it could take minutes for a web page to load and even longer to download files. In the late 80s and early 90s there wasn't a huge demand for bandwidth because, apart from piracy, there were no applications that demanded more bandwidth for faster downloads. Web pages were pretty static, they didn't contain streaming audio, or video, it was just words and pictures, the code that made up web pages at this time was pretty simple there were no rich internet applications like FaceBook, Flickr, MySpace ect... Also there were not enough people on the internet to demand faster speeds but this would change. As software became more popular so too did the quality and size of the software which meant it took longer to download files. Larger files meant it took longer to download which made dialup feel so slow to the point of being useless.

Dial up would also tie up a phone line meaning that incoming calls could not be received, although many people did rent a second phone line for the sole purpose of gaining access to the internet through a dial up modem on one phone line and still receive phone calls on the other phone line. But as technology advanced so to did the size of files which created problems. The other problem with dial-up connections is that a connection would get timed out or the session limit would be reached, a lot of ISPs at the time had 4-6 hour session limits, to keep downloading a file the connection would have to be re-established and the download would have to be resumed or started again if the download could not be resumed. A lot of programs did not support automatic resuming of a download which was interrupted which means the file would have to be

downloaded again from the start. For particularly large files you would have to hope it downloaded before the connection was dropped/timed out but with the size of some files this became close to impossible.

To alleviate this problem a lot of pirate release groups packaged their releases into dial-up friendly size files using compression programs that would not only make a file smaller than its actual size it could also split a large file into smaller parts. An 80 Mb file could be compressed to 60 mb and split into 42 1.44mb files, these files then could be uncompressed in order which would reconstruct the original 80 MB file.

Now users could download a 60 mb file in parts, so it didn't matter if the connection dropped. If a connection dropped while downloading file 25 of 42, a user would just start downloading from file 25 again. It made it a lot more convenient to download a few files each time they dialed a connection rather than having to try to download an 80 mb file at once. This method was a more efficient way of using bandwidth meaning that a user would waste less of their download limit if they were unfortunate enough to have a data limit. This meant a user wouldn't have to keep re-downloading the same data each attempt. This solution was a lot more bandwidth efficient as the user could potentially download more data than was necessary, e.g. a user might download 98Mb of data through wasted attempts when trying to download an 80 Mb file, the other 18mb are failed attempts. If it took the user 4 tries to successfully download the whole 80 mb file and the first 3 times they only downloaded 24, 36, and 61 mb of an 80 mb file on each respective try then that was 121mb of data wasted while trying to download an 80 mb file. By splitting a file into smaller parts a user would waste less bandwidth if they had to re-download only a part of a 1.44 mb file. It was like a discount, if you go shopping and receive 25% off a piece of clothing you would save money, likewise with data, if a user downloads a file that is compressed by 25% then you save bandwidth and would get more data value out of their download limit.

Piracy groups would also release 'rips' to make games and applications easier, more practical and convenient to download. Rips are software titles (games or applications) that has had parts removed, or 'ripped' as in ripped out hence the name 'rips', to make the file size smaller and ergo faster, more practical and convenient to download. Usually features like cut scenes in a game, or extra content that wasn't essential to the software was removed to keep file sizes small. Rips made it quicker, easier and more convenient to download content with a dialup connection. But as the size of files and data grew so did the need for faster connections to transfer more data faster. ISOs would become the next big thing. ISOs were exact 1:1 digital copy of a piece of software, a game, DVD etc... it's like a photo copy of a CD. Since games and software came on CDs it's easier to simply make an exact copy of the CD rather than going to the effort of ripping parts of the software or game. Now all reverse engineers needed to do was crack the copy protection. The problem with ISOs is that they are huge, it's not uncommon for an ISO to be 600mb or more which presents a bit of a challenge to a dialup user, even if they download the 600 mb in 1.44mb chunks it will still take a long time. A faster type of internet connection was needed but there wasn't any practical application(s) that demanded a faster connection at this time.

The term "Web 2.0" was coined in January 1999 by Darcy DiNucci but it wasn't until 2002/3 that the term was really popularised when O'Reilly Media and MediaLive hosted the first Web 2.0 conference. Rich internet, 'web 2.0', applications were starting to be developed that demanded more bandwidth. Applications like Flickr & FaceBook which launched in 2004, YouTube then launched in 2005, and cloud computing (which has been under development for a while and is gaining in popularity) were being developed, these applications would demand more bandwidth since everything was done on the internet (in the cloud, the cloud is the internet) so a fast internet connection would become essential. By this time there were also a lot more people on the internet which meant that the demand for more bandwidth was higher and it was more economically viable to roll out high speed internet services. Enter ADSL, a high speed always on internet connection. The 3 main advantages of ADSL is that it is always on which means a file could complete downloading no matter how long it took or how large the file was. The second advantage is that ADSL is faster than dial up (even the slowest type of ADSL broadband is still about 10x faster than the fastest dial up connection) meaning that more data can be downloaded much faster. Thirdly ADSL doesn't tie up the phone line, so you could be on the phone and surfing the internet at the same time which also made it cheaper, since each time you wanted to get on the internet you wouldn't have to dial a connection which was the cost of a local phone call to dial your provider and you would only need 1 phone line. ADSL and later ADSL2/2+ would make piracy a much bigger problem than it was in the past simply because of the speed of the connection which would let users download huge amounts of data in a short amount of time. Whole movies could be downloaded in under an hour!

Internet connections are only going to continue getting faster with countries like Australia, the US and UK planning to roll out high speed internet to connections to as much of the population as possible, Australia's internet plan, the NBN which will be a FTTH network, will offer guaranteed speeds of at least 12 mbps over a fibre connection, with speeds going up to 25, 50, 100 and even 1000 Mbps. On ADSL and ADSL2+ the maximum theoretical speed is 8 and 24 Mbps respectively. The problem with ADSL/2/2+ runs over outdated and rapidly aging copper infrastructure, the speed of your connection will depend on many factors like distance (the longer your copper cable is from the exchange to your house, i.e. the further you are from the exchange the slower your connection will be), attenuation (which refers to the strength of the signal over

distance, the signal gets weaker and weaker the further it travels so a really long line is going to have a weak ADSL connection hence poor connection speeds), line noise, SNR (Signal to Noise Ratio) Margins, and other factors. So you may or may not get a good stable or even fast connection. Australia's NBN fibre network will offer a guaranteed speed which will mean more data can be downloaded faster, although whether or not a single download from the internet (FTP/BitTorrent/HTTP:, ect...) will be able to saturate the connection is debatable, pirates will be able to move illegal data about faster. But then the NBN isn't just about fast download it's about much more than that but that is a whole other topic for another essay and beyond the scope of this essay. Other countries are also looking at upgrading their network to allow for faster internet speeds, while countries like South Korea and Japan already have access to fibre connections, and the rate of piracy in those countries are over 40% & 20% respectively. Globally internet connection speeds are on the rise and it is only going to aid pirates and piracy.

In the mean time computers and computer hardware has kept, and still is, getting faster and cheaper. The capacity of computer hard drives is increasing (the largest single HDD available right now (in Feb, 2011) is WesternDigitals 3 TB HDD) and the cost per a gigabyte of storage is falling. Portable storage devices like portable HDDs and USB memory sticks as well as CD's and DVD's (and now Blue Ray disks which are set to replace CD's & DVDs although the technology is still new) have become common place making it easier than ever to copy data, carry it about and transfer from one PC to another. Internet access is getting faster and cheaper. All these advancements in technology has made piracy the wide spread rampant problem that it is today by making it cheaper, easier and faster to copy data.

At the end of 2008 it was estimated that there were 1,574,313,184 internet users world wide<sup>46</sup>. The seventh Annual BSA/IDC Global software study found in 2008 the world wide software piracy rate was 41%, that's 645,468,405 pirates who are infringing copyright! And that is just software alone, that's not counting music, movies, TV or any other type of piracy.

In Australia alone movie piracy cost the nation \$1,370 million dollars in sales, (\$193 million in taxes and \$551 million in GDP) and cost 6,100 jobs<sup>57</sup> and that's just in the 12 months up to Q3 2010. Holy calamity scream insanity! IPSOS and Oxford Economics who undertook the study on behalf of AFACT say that these figures are conservative. Imagine what the figures would be if software, game, music and other types of piracy were included, Australia should be bankrupt.

It has to be noted that there is a lot of conjecture as to the accuracy of the findings in a lot of piracy studies. Research and data collection and research methods that are employed are argued to be flawed, like the methods and findings in an Internet Commerce Security Laboratory study, conducted by researchers at the University of Ballarat, which concluded "*that only 0.3% of all files available on BitTorrent are confirmed to be 'legal'*"<sup>65</sup>. The same researchers have been chastised and labelled as "Incompetent"<sup>66</sup>, by the same person, for another piracy study they conducted. The results and arguments on both sides have to be taken with a grain of salt, we have to look at who is behind any study of piracy. A lot of anti piracy groups who have an axe to grind like the BSA, RIAA, MPAA etc... conduct piracy studies then claim that the sky is falling. It doesn't help when the people conducting the studies don't have an ounce of knowledge about how the internet in general works either. The 'war' on piracy really is like a real war there are extremists on both sides, sometimes they have a point other times they are just grinding their axe. It's important to take a step back and look at the motivations of the people who make such claims. One thing is clear, right now it's an argument and arguing isn't going to solve anything until we all start being proactive.

The truth is it's hard to get any accurate data on piracy. The figures I use here are only to help illustrate my ideas. I do not claim that they are entirely accurate. However I will humour the researchers of studies that I use and pretend that they are correct, I'm not going to waste my time arguing about figures. There are more important things to argue about.

The advancement of technology, namely the computer and the internet, has made piracy a big issue, such a big issue that war has been declared on piracy. A war that isn't going to be won, nor lost, a war where the only casualties are the consumer.

To think that piracy can be stopped in it's tracks is plain naive and only shows a gross lack of knowledge about the issues involved with piracy. Piracy can only ever be reduced. One reason why piracy will never be stopped can be attributed to a computers ability to make an exact 1:1 copy of data, also the internet and exponential growth are major contributing factors. In the days before the internet the amount of pirated copies of, games for example, available were somewhat limited by geography. Someone would copy a game for a friend. These two friends were usually in the same geographical region, because it's a bit more difficult to distribute copies over a large geographical region because of the expense involved, as explained before piracy be cost prohibitive unless you had deep pockets, not that this stopped anyone. Floppy disks cost

money, and it cost money to post them. Ingenious pirates managed to game the postal services and posted illegal games and software illegally by re using stamps. There are even spesific postal services designd for posting data on HDDs, CD/DVDs ect... Although illegal software was traded over long distances via BBS's, this method could be prohibitively expensive if the BBS didn't have a local number, or you paid for your phone calls by the minute, although I am sure phone companies made huge amounts of money from pirates who ran up huge phone bills for dialing long distance numbers of BBS's located in other states. The expense of dialing a BBS did limit the spread of piracy to a certain extent, but it never stopped it altogether.

The internet would make piracy a lot cheaper, easier and it would make piracy a much bigger issue. If someone buys a CD and wants to share it via the internet, say via BitTorrent. They would make a ".torrent" file and put it up on The Pirate Bay or any other number of Torrent trackers, one person downloads a copy, then there are two people with a copy of the CD. Those two people then share it with two more people who in turn share it with others, soon there are hundreds if not thousands of copies of the CD floating around the internet. Now the law of exponential growth and the law of accelerating duplication takes over. One copy becomes two, two copies become four, four becomes eight, then sixteen, thirty two, sixty four and so on ad nausea until there are hundreds and thousands of copies in just minutes. It is technically impossible to eradicate all the copies of the shared CD because you would have to find each PC that had a copy of the said CD and the corresponding torrent file then delete those files, it is logistically impossible.

Take a look at The Tunnel, a film released for free and distributed via bittorrent. The film can be downloaded from Vodo although it can be downloaded from other places as well I'm going to use the figures on Vodo to illustrate the point. The film was released on May 19 and at the time of writing (June 1, 2011) it has been downloaded more than 238404 times in 14 days.

To effectively stop piracy, the internet would have to be shut down. While technically possible it's practically impossible, the logistics of such an operation would cost too much in more ways than one. Even if the internet was some how rendered inoperable piracy would still exist because we would still have computers, they just wouldn't be networked which would slow piracy but not eradicate it. Piracy would take place via sneakernet and other ingenious ways that people would invent like *dead drops*<sup>58</sup>. Piracy would become a lot more labour intensive but it would still exist. To completely eradicate piracy we would have to rid the world of every single computer. That is never going to happen because society would collapse if the internet and computers magically disappeared the world's electricity supply would stop and we would be plunged into darkness, air traffic control would stop and plans would fall from the sky, traffic would be thrown into chaos with no electricity to power the traffic lights, the stock market would collapse and money would become worthless. Society world wide relies on the internet, networks and computers to work without them it would be the start of the digital apocalypse. The truth is that piracy is going to be par for the course as long as computers and the internet exist. The best that we can do is to try to reduce piracy.

Debate rages about how to stop or reduce piracy or whether it should be stopped or reduced at all. Some think piracy should be stamped out at all costs, others don't see piracy as a problem and think that there are other more important questions that need to be addressed which may or may not reduce piracy. There are always two sides to any argument. There are plenty of people with vested interests on both sides. As with any war there are always extremists who try to cloud reasonable judgement. To figure out how to reduce piracy we need to look at facts not opinions and ignore the extremists on both sides.

If piracy is going to be reduced then there are two important questions that need to be answered, *how* and *why*. Once those two questions have been answered we will have a clearer idea about how to reduce piracy.

## How?

Granted the question of *how* people pirate isn't as important as *why* people pirate. But it is still an important question to fathom because understanding how people pirate will illustrate why piracy will never be stopped unless the internet and every single computer is wiped out of existence.

It's wrong, not to mention totally naive, to blame the internet alone for the rate of piracy and try to sensor and control the internet. Not all methods of piracy rely on the Internet, although the internet has brought piracy to the masses and dragged it out into the spot light there are plenty of other methods used in piracy that don't rely on the internet. I will explain how there are any number of ways that someone can pirate copyrighted material if the internet never existed. If the internet was never invented computers would probably have still become just as powerful and cheap as they are now, maybe it might have taken longer. Either way piracy would still be a problem, although piracy would probably not be as wide spread and rampant as it is now.

I am only going to look at how pirated material is distributed and not the ins and outs of how it comes to be

available in the first place, that would be a whole other essay. Why people pirate is a more important question to answer so I will only briefly cover how people pirate.

### **Software counterfeiting**

Software counterfeiting is the art of illegally duplicating and selling copyrighted software designed to make it appear legitimate. Usually the illegitimate software comes boxed and the fake, to the untrained eye, is hard to distinguish from the original. Counterfeit software is usually sold cheaply at 'discounted' prices and is usually found at markets, swap meets (computer fairs) and online through auction web sites (like ebay) and other nefarious web shops. The average person would assume they are just getting a great bargain and not have a second thought, little do they know they are purchasing pirated software as the quality of the packaging is often genuine enough at a glance to fool the average person. If the counterfeited software is brought on a web site like ebay or any other web site there is no guarantee that the user will get what they think they purchased, i.e. what was pictured on the web site may not be what they actually get. The user could get a pirated copy, i.e. a counterfeited piece of software.

In 2006 the Microsoft Legal and Compliance team found that of 115 software samples taken from Ebay only 49% were genuine, 39% were counterfeit, 8% was tampered with and the last 4% came with additional software components that were counterfeit or genuine software that had been tampered with.<sup>66</sup>

Some web sites sell software as a backup claiming that it is legal to buy the software because it's a backup copy, which it is not. It is pirated and still illegal to use.

### **OEM unbundling**

OEM unbundling is the practice of selling software that was intended to be bundled with specific accompanying hardware. When you buy boxed hardware from a retail store you sometimes get OEM software in the box. For example a Bluray optical drive might come with an OEM copy of Power DVD. Some people take the software out of the box and sell it on it's own sans the hardware that was supposed to accompany it. While the software is still legitimate it is illegal to sell OEM software. Although OEM unbundling is a bit of a grey area because it is possible to buy legitimate OEM software like OEM copies of a Windows (which is a lot cheaper than the boxed retail version) operating system can be purchased which is intended to be used by system builders (people who build computers for other people) who build the system, install Windows from the OEM media then sell the PC along with the OEM copy of the Windows operating system to the customer.

### **Hard disk loading**

Is when someone installs an unauthorised program, whether it was purchased legitimately or not, on another PC. Hard disk loading is usually illegal unless the software is licensed to be used on more than 1 PC. Sometimes businesses will try to save money by installing a program on all of their machines despite the program only being licensed for 1 PC. Hard disk loading is more commonly practised by a private PC seller to try to entice a purchaser to buy the PC. Most buyers don't have a clue how to set up a PC let alone install programs so it's more attractive to the buyer if everything is already installed for them, it's less they have to think about and do because they expect things to just work, god forbid they actually have to think or learn something new. Sometimes the seller will raise the price of the PC because it has software pre installed, the buyer will usually have no idea that the software is illegal and will pay an inflated price for the PC with the pre installed software. More often than not the PC seller knows what they are doing is illegal and loading illegal software and raising the price is just fast (and dirty) money.

### **Renting**

The problem with renting DVDs, CDs or Games is that a DVD or CD can be copied easily to a home computer with minimal effort. Someone will rent a DVD, CD or console game then go home and copy it to their computer, take the DVD, CD or game back and get more and do it all over again. It's faster than downloading, it saves bandwidth and is cheaper than buying the product legally. If the internet didn't exist then this sort of 'rental piracy' would most likely be more common assuming that video rental stores are still around.

### **Sneakernet**

*Sneakernet is a method for transferring electronic information, especially computer files, by physically couriering removable media such as magnetic tape, floppy disks, compact discs, USB flash drives, or external hard drives from one computer to another. This is usually in lieu of transferring the information over a computer network.*<sup>49</sup>

USB memory sticks, CDs/DVDs, and portable Hard Drives are usually loaded with copyrighted material and transported to another computer where the data is then copied to.

Sneakernet is used and is ideal for transferring large amounts of data when it would be impractical to transfer the data over other types of networks. Where two networks may not be compatible Sneakernet may be used to transfer data between these networks. Infact Amazons Simple Storage Service (Amazon S3) recommend sneakernet, although they call it AWS Import/Export, for transferring large amounts of data<sup>59</sup>. There are postage services specially designed for transporting computer equipment.

Sneaker net is often used to illustrate the trade off between latency and throughput.

Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway<sup>60</sup>.

Sneakernets can achieve massive throughput but at the cost of extremely high latency. Consider person A had a 4.7 GB DVD of data that person B wants. Person A could throw up an ISO of the DVD online so that person B could download it over the internet. Latency over the internet is usually measured in milliseconds but even with a modest, lets say they have a 512 kbps, connection and they can download the file at 50 kB/s it could take a day or longer to download the file. Let's say that Person A lives an hour away from Person B. Person A could burn a copy of the DVD and deliver the data to person B in an hour. The latency is an hour but the throughput is about 1305 kB/s.

In theory a Boeing 747 can hold 595,520,000 Gigabits of data on 1,488,800 Blu-ray DVDs. Assuming that the Blu-rays are cased in slim jewel cases that each hold 1 Blu-ray. The time (latency) to travel between point A and point B is 4.46 hours, but the throughput is 37Tb/s! Try doing that on any network right now<sup>61</sup>. I'm sure it will be possible oneday, just not right now.

And there are plenty of real world examples of sneakernet usage. In the UK on September 9 a race between a pigeon and a broadband connection took place. The race was to see who could deliver 300mb of data faster, a pigeon or a broadband connection. *An hour and a quarter later, the pigeons had reached their destination in Skegness 120km away, while only 24% of a 300MB file had uploaded*<sup>62</sup>. Google uses sneakernet<sup>63</sup>, and Netflix effectively uses sneakernet by mailing out DVDs to customers.

Sneakernet is the best way to hilight the fact that if computers existed without the internet then piracy would continue via sneakernet.

### **Softlifting**

Purchasing a single licensed copy of software and loading it onto multiple computers contrary to the license terms. For example, sharing software with friends, co-workers and others. Even if the CD/DVD (or what ever medium the software was distributed on) is not copied and distributed (given to others) it is still being distributed on other computers simply by installing it.

A lot of software usually only comes with a license for one PC so if you want to install the software on another PC you would need a licence so the software can be used, depending on the type of software volume licences can be purchased to allow the software to be used on more than one PC. A lot of the time there is nothing stopping some one from installing the software on another PC. This type of piracy is more rife amongst big businesses and corporations where multiple PCs are needed for staff. It's an illegal way to cut costs.

### **Internet piracy**

Making unauthorised copies of copyrighted material available to end users via the Internet. Most people think of the WWW as the internet although the internet is much more than just the WWW. For the purposes of this section the word 'internet' refers to the World Wide Web.

The WWW is one of, if not, the biggest enablers of piracy since it helps people find information on piracy i.e. how to find and download what they want. as well as programs that let them pirate copyrighted works, There are numerous ways people can the internet for piracy the WWW is just one of the ways that people use the internet for piracy. It could be argued that any one that can type what they are looking for into a search engine is capable of piracy. Peer to peer (P2P) programs like Napster, Gnutella, Audiogalaxy, KaZaA, Morpheus, and protocols like BitTorrent ect. Are found on the WWW. These programs make downloading content a lot easier. If it were not for the WWW then piracy would be much less of a problem than it is today. The WWW enables people to find information and programs to help them download what they are looking for. It helps them find torrents and share illegal data.

Pirates don't usually 'rip' a game or piece of software now that high speed internet connection with large download limits are available at affordable prices, they will release the whole game or application minus the copy protection/DRM, box, manual and other miscellaneous bits and pieces that might come with a boxed

piece of software. They are called ISOs and are an exact 1:1 digital copy of the original game, application, CD, DVD etc...

But before a user can download a game, application or anything else there is a lot of work that goes on behind the scene before anything is made commonly available. It has to be released and distributed. There is a highly secretive group of insiders, hackers, crackers, reverse engineers, packagers, distributors and couriers that make pirated applications, games, movies etc... available. This collective is called the Warez Scene or more often just the Scene. The scene is a collective of people that operate under the cover of darknets, dark networks or darknets are parts of the internet that are closed off and to all intensive purposes don't exist except to all but a handful of individuals who know that the network exists and they are usually highly protected by strong encryption. There is a hierarchy of specific channels that a release goes through before it is made available to the general public:

1. The insider.

The insider is the person that has access to the game, application, movie, ect. before it is released. An insider can also be an individual or a collective of hackers that hack secure servers to illegally gain content like the latest game, application, movie etc... before it is released. Once an insider has anything of value they leak it/pass the content on to release groups.

2. The release group

The release group is responsible for converting (removing any copy protection, compiling source code etc...) and packaging the title so that it is easier to distribute and easily downloadable. Once the release is ready to be distributed it is then passed on to the distributor.

3. The Distributor

At the top of the piracy food chain is what are called top sites, these are highly secretive sites that receive the latest pirated titles. Once a release is dropped on a top site this is when the avalanche begins courtesy of couriers. Once a release is made available on the top sites it can take only minutes before one file becomes 30 files becomes 3,000 files becomes 300,000 etc... Thanks to couriers.

4. Couriers

Couriers are the worker bees of the piracy scene and they are responsible for distributing a release to many other lower level dump sites, and then to P2P networks. The pay-off is props from their peers and credits redeemable for goods on upper levels of the pyramid.

5. The general public

After the courier has done their job the file has already been copied, tens, hundreds, maybe hundreds of thousands of times. The general public are at the bottom of the piracy food chain as they rarely get access to top sites, or even know that these top sites or the scene exists since they are hidden under the darkness of darknets.

Once a release has passed through the scene it is available to the general public who have a number of ways available to download illegal via the use of P2P programs, BitTorrent, FTP sites, IRC, Usenet ect.

Then there are warez websites. Warez web sites like PhazeBlog, phazeforums, WarezUSA, HQ-Uploads, XtremeSharez, WrzBoard and many others can be found by anyone who can type 'warez' into a search engine. They appear all over the internet like a rash. There are even Warez search web sites, they are search web sites like google except they are specifically for Warez. Some 'Warez' sites offer direct downloads of software, a lot of warez sites will require you to sign up and only after registering is a user allowed to download what they want. This sign up usually guarantees spam to flood into a users email inbox if they are not wise enough to use a throw away email like mailinator or a similar service, and that's if the system is silly enough to allow users to use such throw away email accounts. Viruses and other unwanted malware is another risk that users face when using warez sites. In 2006 Microsoft sponsored a study that was carried out by IDC on "The Risks of Obtaining and Using Pirated Software", the study found that "25% of the Web sites we accessed offering counterfeit product keys, pirated software, key generators or crack tools attempted to install either malicious or potentially unwanted software."<sup>64</sup> and "11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from

*peer-to-peer networks contained either malicious or potentially unwanted software.*<sup>765</sup>

Other web sites describe themselves as “trading” communities like craigslist and iOffer.com are used by software scammers to distribute their counterfeited software and turn a profit. Then there are web sites such as RapidShare, Megaupload and Hotfile, which allow users to upload files to make them publicly available to anyone, are used to house files then links to the files hosted are distributed via email, IM, or links on forums and other web sites like blogs.

Web sites like eBay are used by millions of people to buy and sell goods. These goods include hard copies of counterfeited software on CD/DVD. It is hard for people to know that they are buying counterfeited software because they can not inspect the goods for signs of counterfeited software before they make a purchase, and even if you know what you are looking for it can be hard to spot a fake.

### **Peer to Peer (P2P)**

Programs like Napster, Gnutella, Audiogalaxy, KaZaA, Morpheus, BitTorrent ect. These programs work by sending data from one PC (a peer) to another PC (another peer) via a distributed network meaning that there is no central server to shut down which makes controlling or even totally shutting down P2P networks close to impossible because you would have to shut down hundreds of thousands of computers, which are usually private computers in peoples homes. The whole internet would have to be shut down to effectively eradicate P2P file sharing, which is neither possible or a real option.

Internet piracy and BitTorrent are the most common ways that people pirate copyrighted material.

BitTorrent indexing web sites are used to facilitate and obtain and sharing of illegal software, music, movies, TV shows etc. They do not contain the files they merely describe where the file can be found via .torrent files. *In Europe the Middle East and Australia P2P traffic consumes anywhere between 49 percent and 89 percent of all Internet traffic in the day. At night it can spike up to an astonishing 95 percent*<sup>47</sup>.

There are also private networks known as Darknets that are not visible or accessible to the public and are protected with encryption. Generally dark nets are set-up by 2 or more users that know and trust each other. They are set-up to transfer data usually pirated software or any other kind of nefarious data that is not generally considered legal.

### **File Transfer Protocol**

FTP is another method used for piracy. File Transfer Protocol (FTP) is a standard network protocol used to exchange and manipulate files over a network and was originally designed to:

- To promote sharing of files (computer programs and/or data).
- To encourage indirect or implicit use of remote computers.
- To shield a user from variations in file storage systems among different hosts.
- To transfer data reliably, and efficiently.

Although FTP was never designed for sharing illegal data it is well suited to piracy. FTP is built on a client-server architecture which means you have an FTP server, a PC that hosts the files (the PC will be running some sort of FTP server software to turn it into an FTP server) and the client which is a bit of software on a remote PC that is used to access the FTP server.

An FTP server can be as simple as a home PC with an internet connection and FTP server software used to turn the PC into a server.

### **Internet Relay Chat**

IRC is mainly designed for group communication in discussion forums, called channels but also allows one-to-one communication via private message as well as chat and data transfers via DCC (Direct Client-to-Client). IRC networks have large numbers of channels dedicated to piracy that contain bots or scripts that turn the IRC client into a file server which use the Direct Client-to-Client (DCC), a protocol built into IRC that is supported by many IRC clients, to transfer files. IRC files servers are scripts that automate file sharing.

### **Usenet**

Conceived in 1979 and publicly established in 1980 Usenet is a worldwide distributed Internet discussion system. Usenet was *Originally built on the "poor man's ARPANET," employing UUCP as its transport protocol to offer mail and file transfers*<sup>48</sup>. The ability of any system that can store and serve files can be miss used for copyright infringement, Usenet is no exception. Usenet is typically accessed via a Usenet client used to browse topics, read topics, and to download files. Although Usenet is still in operation today it's

popularity has declined.

### **Cracks, Patches & Keygens**

*Cracks, patches and key gens (or key generators) are used to modify software and bypass protection such as evaluation periods that stops software working after a period of time or reduces functionality or simply produces nagging screens each time the software is started. Cracks, patches and serial key generators that are available for free can unlock features that are normally unlocked by purchasing a licence which gives the user a serial key that they enter which then unlocks features, turns off nag screens or otherwise give the user full functionality of the program. Some software requires that it be registered by purchasing a licence in order to use it, when you purchase a licence you get a serial that you enter which entitles you to use that piece of software. Cracks, patches and key generators bypass these security systems.*

*An IDC study has found that 59% (of 94 samples taken) of downloaded keys, key generators, and crack tools downloaded from P2P networks contain malicious or potentially unwanted Software<sup>67</sup>. And that only 11% (of 116 samples taken) of the afore mentioned software that was downloaded from web sites contain malicious or potentially unwanted Software<sup>68</sup>.*

If the internet disappeared tomorrow, piracy would slow down dramatically but it would still continue via methods that don't require the internet, piracy would continue via Sneakernet, HDD loading, OEM unbundling, softlifting, and software counterfeiting. Computers would also have to disappear along with the internet which is never going to happen given how much society relies on computers alone let alone the internet. Now that we know what methods pirates use it's easier to see why piracy will never be stopped, ever, it can only ever be slowed down. Now the question now becomes why? Why do people pirate?

## **Why?**

Addressing only the methods used in piracy would ultimately be ineffective, it would be like treating the symptoms of a problem and not addressing the root cause of the problem. If the reason why people pirate is solved then *how* they pirate will become less relevant because people wouldn't be pirating anything in the first place instead they would be making legal purchases or just not pirating to begin with. Prevention is better than cure as they say. The question that needs to be asked and answered to try to prevent people turning to piracy in the first place is why? Once we understand why people pirate we will understand why it will only ever be slowed down and never stopped.

We know that the uptake of super fast ADSL internet around the world has made piracy a much larger issue than it once was, super fast connections make it easier to download huge amounts of data (movies, music, TV shows, games, applications, ect..) faster than ever before. P2P networks have exploded in popularity and the internet, more specifically the World Wide Web, makes it easy(er) to find almost anything you want you want.

Just because someone has a super fast ADSL connection doesn't mean they are going to pirate copyrighted material. The technology is there whether people choose to use it illegally or not is up to the individual. A super fast internet connection can be used for lots of other legitimate reasons as can P2P protocols like BitTorrent, but why do people still choose to use their internet connection illegally to download copyrighted material? What's the motivation?

Some people will always take what they can get for free because they can. Why pay for something when you can get it for free? Others do it because it's available and convenient, it's easier to pirate than it is to purchase it legitimately. Some people pirate software because they believe the quality of the software is not worth paying for "*I bought RA3 for 35\$ on sale, and regretted every dollar of it*", this infers that people would buy software if it were of better quality, which leads to another reason price. The price is often way too high for what you get. A lot do it because of Digital Rights Management (DRM)<sup>2</sup>. Others, a small minority, pirate for other reasons, hate of capitalism or intellectual property. There are many reasons why people pirate and to make it even more complicated people usually pirate for more than one reason.

### **For the challenge**

Piracy groups (groups like CDA (Compress Da Audio), CORE (Challenge of Reverse Engineering), uCF (uNITED cRACKING fORCE) etc...) compete with each other to crack (reverse engineer copy protection) and release software (games & applications), music, films (DVDs) ect... before it's released to the general public or by other groups. They see it as a challenge. The challenge is to reverse engineer the copy protection and release the software (games & applications), music, movies etc... faster than other groups. What they gain is popularity, notoriety, the crackers in the group do it to gain knowledge, it's an intellectual challenge.

## **Region locking / Territorial distribution**

Region locking / Territorial distribution is when media (DVDs, TV, online videos, etc...) is locked/blocked or exclusively distributed in/to a specific region. DVD region encoding is a common practice intended to make sure that DVDs purchased in one region can not be played in another region. For example a Region 1 (USA & Canada) encoded DVD is not intended to be sold or played outside of that region that it was intended for, that is it can not be purchased or played in region 4 (Latin America & Australia).

The entertainment industry use DVD region encoding to maximise profits by staggering the release dates of DVDs. For example movies are typically released in America and Canada first, then Australia and Japan 6 months later, followed by Europe 12 months after US release. DVDs are released in the USA first because that is where the most profit is and the DVD can be sold for \$20 for example, then the DVD is released in Australia and Latin America because there there is less profit to be had in those regions because the population in those regions is lower than other regions so they raise the price to \$30. Staggering the release of DVDs across different regions enables price fixing to maximise profits because a DVD can be sold for more in one region than it can in another.

In practice region encoding/locking fails epicly as there are a number of ways to bypass or break region encoding for DVDs and hardware DVD manufacturers make DVD players that can play DVDs from any region, this is what they rely on to make sales. DVDs can also be imported form other cuntries/regions.

Region encoding/locking actually promotes piracy as it is simple to rip a DVD to a file that can be played on any computer or device anywhere in the world. For example a popular movie you want to get on DVD (that you are willing to pay for legitimately) is released in America, it's not due to be released for another 12 months in Australia, but you really want it. Hours after it is released in Amrerica someone has ripped the DVD to an ISO file and posted it on a number of Bit Torrent tracking web sites so you go download it anyway<sup>4</sup>. All you need to do is hit your favourite Bit Torrent web site and download the DVD image and burn it to DVD. Now you have an exact copy minus the artwork of course but who cares you got it cheaper and quicker than waiting for the official release simply because you could not buy it although you did want to and did intend to buy it legitimately. If DVDs were released worldwide on the same day movie piracy could be reduced dramaticly. Likewise if DVDs were released across all regions, i.e. there were no regions at all, movie/DVD piracy wouldn't be such a big issue.

The same applies to TV shows that are some times never aired outside a particular country, but with digital TV and computers it is easy to record a TV show and share it on the internet.

Producers are crying foul of people taping and sharing TV with the advent of computers, the internet, HD TV and the ability to remove adds, there seems to be little reason to by the DVD of TV shows.

## **Digital Rights management (DRM)**

Digital Rights Management (DRM) refers to access control technologies used by publishers, copyright holders, and hardware manufacturers to limit usage of digital media or devices.<sup>5</sup> DRM attempts to control how media is used and on which devices/platforms the media can be used on, it does this by by preventing access, copying or conversion to other formats by end users.<sup>6</sup> DRM can be applied to all sorts of media, music (Digital files like MP3s & CDs), DVDs, software (games and applications), documents. DRM can be bypassed or cracked and released for download on the internet, or copied and shared/sold.

Another reason why users pirate is because DRM restrictions can cause all sorts of problems. For example some major record labels dabbled in applying DRM to music CDs which could cause problems like computers to crash, or CDs would not play in all CD players because they lack the CD logotype found on discs which follow the standard known as the Red Book standard. DRM can also create a severe security vulnerability, like the Sony DRM known as XPC. Security researchers have shown that the XCP technology was designed to have many of the qualities of a "rootkit." It was written with the intent of concealing its presence and operation from the owner of the computer, and once installed, it degrades the performance of the machine, opens new security vulnerabilities, and installs updates through an Internet connection to Sony BMG's servers. The nature of a rootkit makes it extremely difficult to remove, often reformatting the computer's hard drive is the only solution guaranteed to get rid of the root kit. When Sony BMG offered a program to uninstall the dangerous XCP software, researchers found that the installer itself opened even more security vulnerabilities in users' machines.

Sony's DRM software only had a limited ability to prevent copying, as it affected only playback on Windows computers, not on other equipment. Even on the Windows platform, users regularly bypassed the restrictions. While the Sony DRM technology created fundamental vulnerabilities in customers' computers, parts of it could be bypassed by holding down the "shift" key while inserting the CD, or by disabling the autorun feature. In addition, audio tracks could simply be played and re-recorded, thus completely bypassing all of the DRM (known as the analog hole). In the end Sony had to refund customers or offer free downloads. DRM can and does lead to increased rates of piracy, take Spor for example. The DRM imposed on users in Spore lead users to pirate the game making it the most pirated game of 2008<sup>7</sup> &<sup>8</sup>. People pirated Spor to get away from DRM. DRM can be applied to many types of media, if it can be applied it will. It will also be

cracked and pirated. If you buy something then it is yours and you should be able to do what you want with it, for example if you buy an MP3 you should be able to copy it to and play it on any device you want. DRM promotes piracy because users know that if they download a game, mp3 or movie that has the DRM cracked then they can simply play it and not have to deal with over intrusive DRM that they would otherwise have to deal with if they brought the product from the store. Why would you pay for something knowing that you will be restricted in what you can do with your purchase without having to deal with over intrusive DRM. It's simply easier to pirate it because the pirated version has no DRM.

### **No demo/trial version**

People will often pirate a piece of software because it has no demo/trial. A demo or trial is a short version of a game or a cut down version of a software title that has limited capabilities, usually it is enough to give the user a reason to buy the full version. Demos and trials are most common in the gaming and software industry. If there is no demo then people will resort to pirating the full version to try it instead if they want to try before they buy. People don't buy things then decide they don't want what they brought. How do people know they want a particular software or gametitle? They have probably used or played it before. This is highlighted in the gaming industry when publishers don't release a demo of a game so people will pirate the full version just to try it. Then if they like it they will probably keep playing it and not bother buying the full version. Or they will get bored of it and maybe delete it or just not play it at all. It would seem to be a fairly black and white issue. It is fairly commonly cited, by gamers in particular, that people will pirate a game because it has no demo version available. Many users share the same opinion like DirtyFlorist who commented on an article about piracy, *"i downloaded that Modern Warfare for PC. You know why, b/c the publisher/developers didnt give me a free trial to play the game before i bought it. I dont buy any game before playing it, and if they want me to buy it, they should let me demo it first."*<sup>69</sup>. Shane39199 commenting on the same article posted *"i pirate games if theres no demo or trial"*<sup>70</sup>. In 2008 Cliff Harris a 38 year old Game Designer and programmer from the UK put out a "Genuine call for emails from pirates"<sup>71</sup> because he wanted to know why people pirated his games. What he got was a more general response about why people pirate in general. A recurring reason was lack of a demo, Preston commented that *"I do it mainly because of quality or no demo. If I can't easily gain access to a demo, I can easily gain access to the full game."*<sup>72</sup>, jeff said he pirates when *"...no demo exists..."*<sup>73</sup>, likewise scott says that *"...the main reason I would pirate a game is: 1) just want to try a game but no demo exists..."*<sup>74</sup>, ic commented that *"I too feel that for some games there are no Demos, so pirating becomes a "try before you buy" type of thing."*<sup>75</sup>. However a demo can be a bad thing if the demo is too limited as the commenter known as ic also said that *"some Demos are way too limited."*<sup>76</sup>, another commenter, squinty, wrote *"Demos are usually very short and don't give you a true feel of the game, since most companies may put the best levels into that demo while the rest of the game blows."*<sup>77</sup>. A commenter called Woffie says *"The reason why I download games from suspect (read small and unkown) companies is that theres either not a Demo or the Demo was too short."*<sup>78</sup>, he also goes on to say that *"Demo's? They are spoiling the plot usually, they are way too short and they are usually just almost as big as the full software not to mention they usually lock out several features."*<sup>78</sup>.

### **Quality, pricing and general errors**

It's understandable that school kids with no income would pirate games/software/movies/music ect... they simply can not afford to purchase a legitimate copy of a game or application, movie,, music ect... But then why do people with an income, who can (if they choose to) afford to purchase games/software/movies/music ect... pirate instead? Usually because the asking price is too expensive. Something is only worth what someone is willing to pay for it. Games and applications are a popular target for pirates, what makes games and applications so popular to pirate? Because they are so expensive. But what makes games and applications too expensive apart from the time and effort that goes into making games and applications? Maybe it's just a perception that games and applications are too expensive. What makes them seem too expensive and lack of value for money? Why do games and applications lack value for money? People choose to pirate because they feel that their hard earned money is not worth spending on a product that is not worth the asking price to them. For example if you purchase a game from a retail shop the price will certainly be inflated to cover staff wages, rent and other expenses.

In the afore mentioned blog post "Genuine call for emails from pirates" more than 90/300 people commented that they pirated games because of price, because the price is too expensive. As commenter rd put it *"i do some pirating but purely as a try before i buy or in the case of the cinema before i go and pay as im a student living in the uk where the cinema is £8 a new game is £30-£50 and dvds/bluerays are £15-£40+. so being a student i cant afford to go out and spend my money for the chance that i might not like it etc"*.

Consider this scenario. You read about a game that sounds awesome, so awesome that you immediately want to drop some of your hard earned cash on it. So you google it and find that it is available for \$10 (probably a bit less with the economy the way it is and exchange rates so that's even better this game looks

so cool you just have to have it) on an online distribution platform that allows you to purchase and download game(s) the instant the game(s) are paid for. So you hit up steam and try to register, but alas you get an error informing you that "Your account creation request failed, please try again later.", you try again later, a few times to no avail. You really want the game so rather than paying for it you hit up your favourite torrent search engine and search for the game (the one you want to purchase legally but can't) and his search, and bingo! You have a list of sources longer than your arm where you can download that game for free. So you download the game, in less than half an hour you have the game downloaded, installed and are playing it for a little extra effort and you have also saved some money.

The above scenario is not so far fetched. This happens in the real world, not with just games but TV shows:

*Last week, I tried to buy an episode of a TV show from the iTunes Store. It didn't work and there was no error message. Thinking the download had corrupted something, I tried again and the same problem occurred. (I learned later that I needed to upgrade Quicktime.) Because I just wanted to watch the show and not deal with Apple's issues, I spend two minutes online, found it somewhere for free, and watched the stolen version instead. I felt OK about it because I'd already paid for the real thing \*twice\*, but in the future, I'll be a little wary purchasing TV shows from iTunes and maybe go the easier route first.<sup>2</sup> this is something that could have been avoided if an error message advised the customer that they needed to upgrade their version of Quicktime.*

Yours truly has pirated a game because of an error. I had purchased Mirrors edge from Steam when it was on sale. I played and loved the game, I finished the entire game and was still wanting more. I discovered that there was a map pack available, but it was only available through EAs online shop. I was a bit cautious because I wasn't sure that the EA online shop version of the map pack would be compatible with the steam version of Mirrors Edge, there was no reason why it shouldn't be unless EA made it so in an attempt to make a profit. So I went looking to see if it would be compatible, but nowhere on the purchase page did it mention that the map pack wasn't compatible with the Steam version of Mirrors Edge, that was good enough for me because surely EA would be responsible enough to specifically mention that the map pack is only compatible with the downloaded version from the online EA store or a store brought version of mirrors Edge. In hindsight I should have checked on the Steam web site too, but I didn't. So I gave EA my money and I proceeded to download and install the map pack which is essentially more levels for the game. However there was only 1 problem, the installer started throwing error messages at me. It didn't take long for me to figure out the map pack wasn't compatible with the Steam version of mirrors Edge. After that I spent half of the evening looking and finally came across a post, one small post that only had a few replies, that stated that the map pack wasn't compatible with the Steam version of Mirrors Edge. By this point I was livid as I had no way of getting a refund because EA choose not to refund digital downloads. So I was poorer for the experience. After my anger had subsided I downloaded an illegal version of Mirrors Edge so I could pay for what I had legally purchased. However I never installed the illegal version of Mirrors Edge or even played the map pack because I was over EA. I have since sworn to never purchase anything that EA has anything to do with. If they release a game that I really want to play I'm going to pirate it, they are never getting any more of my hard earned money ever again. Now I avoid EA games like the plague and tell everyone I know about the problem I had with the Steam version of Mirrors Edge and the map pack. I'm sure they would have known that the map pack, if downloaded from their web site, wouldn't work with the steam version (I assumed it would look for, find and install the map pack into the ME folder in my Steam games folder) and issue a note on the store page saying something like "Please be aware that this map pack will only work with the retail or EA version of Mirrors Edge". Anyway it's happened and left me with a sour taste in my mouth.

### **For profit**

Softlifting, OEM unbundling, Hardrive loading are forms of piracy that is more profitable than casual/internet piracy. Some people use piracy to make money by selling illegitimate (counterfeited) software to unsuspecting users. Hard drive loading is used by system builders as a deal sweetener to get people to purchase their systems. Hardware can not be pirated, software can. Software can cost as much or even more than a single piece of hardware or a complete PC and even then you don't own the software, you only own a licence to use the software. A system builder can get access to cheap/free software, pirated software. Software that they can say is legitimate and use it to raise the price/value of a computer to cover the hardware costs and to net them more profit without having to spend extra money at all. Lets say a system builder has a PC that cost \$1285 to build, the system builder could install an illegal copy of an operating system, lets say Windows Vista, that they downloaded for free, and raise the price of the PC to \$1400. They didn't pay for the copy of Windows but they still raised the price and without having to spend any extra money they netted a profit of \$115. It's usually small system builders that would take part in the practice of hard drive loading for profit. The profit made can then be spent on other things, maybe more hardware or other things like entertainment or rent or bills. Sounds far fetched? Handii , a Queensland based manufacturer of tablets has been caught using illegitimate copies of Windows 7 Professional on their tablets.

They have agreed to settle for \$70,000 which is most likely a lot more than they would have spent on legitimate copies of Windows 7 Professional<sup>92</sup>. Whether they knowingly took part in piracy or not it is hard to tell and may never be known, but the point remains that even corporations participate in piracy. Even record labels have been accused of piracy by not paying royalties to artists. Sony Music Entertainment Canada Inc., EMI Music Canada Inc., Universal Music Canada Inc. and Warner Music Canada Inc. have all been accused of not paying royalties to artists for over 300,000 songs dating as far back as the 90's. The defendants have settled for \$50.2 million<sup>93</sup>.

### ***Because it's not available any more***

Software, more notably games, music, DVDs, ect... have a limited life. They are sold for a certain amount of time then once the product is no longer commercially viable (i.e. not enough people are purchasing a product to justify the cost of its production & distribution) it is abandoned and you can no longer purchase it any more, everyone has moved on to the next big thing. Just because it's not available in the shops any more doesn't mean that it's not available at all, it's probably available online. If you can't buy it in the shops but it's available online for free what are you going to do? Most people would download it. Then there is the whole grey area that is abandonware. When a game or software title is no longer sold, supported, or actively developed it becomes abandonware, although the exact definition of abandonware does vary. The problem with abandonware is that just because the software/game can not be purchased any more it is still technically illegal to download it because usually the copyright has not run out and probably will not run out for a long time to come, copyright lasts 50-70 years in most countries<sup>10</sup>. Thus if someone downloads the software title or game they are pirating it/breaking the law/infringing copyright. If the software, game, CD, DVD, ect... were still available for purchase then it could be purchased and people wouldn't have to resort to piracy.

### ***Because they can***

The fact is that some people will always take what they can get for free if they think that they can get away with it, if the risk of being caught is negligible. Because it's easier, sometimes faster, than going down to the shop. There is also the belief that if it's found on the internet then it must be free.

Money that isn't spent on software (games and applications), movies, music, DVDs, CDs ect is usually reinvested elsewhere in the economy, like paying for a fast internet connection with big download limits to download all those games, TV shows, DVDs, software titles ect, or on computer hardware like HDDs to store data, or blank CD/DVD's to backup all of the pirated games, software, movies, music ect... Instead of purchasing that new game at \$99 the user might pirate the game and spend the money on a new video card to play that same game that they just pirated.

## **Risks, consequentness & effects of piracy**

Besides risking getting caught there are other reasons to try to minimise piracy. The probability of getting caught is pretty low but it is still a possibility. If you are caught you face fines and possibly jail time. There have been cases of individuals being caught and fined but these cases are few and far between, but there is evidence that copyright holders are changing their tact and chasing bigger fish like ISPs instead of individual file sharers. I will argue that there are worse risks, consequences and effects of piracy than loss of money or being caught.

The most obvious consequence and most talked about effect of piracy is loss of revenue/profits and jobs. Piracy cost the film industry \$6.1 billion in 2005, according to the Motion Picture Association of America<sup>12</sup>. In the UK, Jupiter estimates that £180 million is lost annually in the music industry alone<sup>13</sup>. Worldwide losses from [software] piracy [alone] increased 20%, or more than \$8 billion from 2006 to 2007 according to the IDC<sup>14</sup>.

Piracy doesn't only cause loss of profit to developers/producers, it also costs in terms of lost jobs & earnings, and lost tax revenue. In 2007 Australia spent close to \$23 billion in IT (Information Technology - hardware and software), which accounted for 3.0% of gross domestic product (GDP), and supported more than 23,500 IT companies that employ nearly 178,000 employees. The spending also helped generate \$10.5 billion in IT-related taxes<sup>15</sup>. IDC predict that a 10% reduction in piracy could create 3,929 jobs, \$1.9 billion in local industry revenues, and \$438 million in additional tax revenues<sup>15</sup>. In 2007 in the US alone piracy costs \$58.0 billion a year, 373,375 jobs and \$16.3 billion in earnings, and costs federal, state, local governments \$2.6 billion in tax revenue<sup>11</sup>.

While the BSA, MPAA, RIAA and others talk about lost revenues, jobs, taxes etc... There are other consequences of piracy.

## **What you don't get**

When you pirate a game, software, music, DVD ect... You get nothing else like manuals, CD notes, support, updates ect... There is a lot of potentially important things that users miss out on.

Packaging isn't an issue or a consideration for most people, least of all pirates, although less packaging is better for the environment, it's not good for the computer and software industry, the economy or jobs. The pros of piracy and the benefits of piracy to the environment don't outweigh the cons. Besides there are better ways to save the environment but that is a whole other can of worms. Packaging serves to keep the CDs/DVDs that the software is on and the documentation together and to help sell the software so it does serve a useful purpose.

When software is downloaded not only does it come without the packaging, it also comes sans manuals and documentation. A lot of software publishers have a lot of online documentation and self help web sites, then there are the third party web sites and forums where people can get unofficial help so official help and documentation isn't seen as much of a loss to pirates.

Pirates also miss out on phone support, but again pirates don't much care for phone support because there is plenty of support online.

More importantly free upgrades, patches and updates that fix security vulnerabilities in the software as well as fix bugs and add new features aren't included with pirated software. It's important to keep your software as well as your operating system fully up to date with patches to keep it secure, insecure software is one of many vectors for attacking a system, look at the security issues Adobe has had with their Acrobat software. Adobe systems have released many patches to fix security vulnerabilities for the Adobe Acrobat Reader software to fix issues that have been found in the software. Granted Adobe Acrobat Reader is free but imagine if it wasn't? There would be potentially hundreds and thousands of people running insecure software that would make them vulnerable to attack. If someone is using illegal software they are not likely to care about updates and security patches that will make their system more secure until something happens, like the browser hijacking problem that I mentioned at the beginning of this essay. Additionally if you try and register a pirated game or application you could risk being caught.

Customers might not always receive what they pay for if they purchase software if they purchase it from anywhere else other than authorised dealers. There are other places where software can be purchased like online auction sites, trading sites and other web sites, and at markets.

If the software is brought at a market or online there is a good chance the software may be counterfeited. Counterfeited software is usually altered to bypass any copy protection. The problem when software is altered is that it could break the software, or other things could be included like viruses, key loggers, trojans, worms or any other type of malware and the user will likely have no way of being able to tell until something happens. Also profits from counterfeited software, DVDs, CDs ect... could possibly be funding criminals.

There is even more risk when purchasing software online from a nefarious web site. The software may arrive incomplete, i.e. no packaging or manuals. The picture on the web site might show the packaging, CD, manuals and documentation but because it's online there is no way to verify that is what will be received. The software could be a pirated version burned to CD/DVD with the title scrawled in permanent marker on the CD or DVD. Even worse it could not arrive at all and someone has your money and credit card details if a credit card was used to pay for the software. Not only do they have your money, and maybe credit card details they also have some of your personal information like your name and address which could help criminals steal your identity. Purchasing software from web sites can be dangerous as you could be willingly handing over personal information and financial details to criminals, information that could be used to help steal your identity and/or drain your bank account.

## **Security**

Getting what you want for nothing isn't always free. Getting caught and fined or in some cases jailed for downloading copyrighted material is only one risk that users face.

One finding in the 2010 United States Government Accountability Office study titled **INTELLECTUAL PROPERTY: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods** that found that *“Counterfeit or pirated software may threaten consumers’ computer security. The illegitimate software, for example, may contain malicious programming code that could interfere with computers’ operations or violates users’ privacy.”*<sup>89</sup>

What some people don't realise is that piracy is a threat to not only their security but other peoples security as well. One of the most common ways people get infected with viruses, worms, trojan horses etc is by downloading questionable content like cracks/patches and serial key generators from what may not be such

a legitimate/reliable source. Just visiting such a questionable web site is enough to infect a PC, they are called drive by downloads where a person only needs to visit a web site with an insecure web browser, like IE 6, which silently downloads and installs malware on a users computer. Cyber criminals use piracy and exploit it for their own gain and nefarious purposes by injecting files with malware, usually infecting the most popular software titles since they are the most highly sought after titles. It makes more sense to infect highly popular software because more people want what is popular and the more people that download and install a piece of infected software means more malware infections which is what cyber criminals want so they have more opportunities to destroy a system, use it in a bot net to launch attacks against their targets, steal information or do what ever else that they want to do. Viruses & malware can range from the annoying to highly destructive, they have the potential to not only destroy your data they can also exploit your personal information stored on your PC like credit card information, banking details and other personally identifiable data that could be used to steal your identity. Piracy has been identified as a cause for cyber attacks in South Korea where hackers have attempted to disrupt presidential office, foreign ministry, intelligence agency and US military websites, *"The country's National Cyber Security Centre said it had seen signs of a "denial-of-service" attack"*<sup>79</sup>. According to The BBC, AhnLab claims that attackers *'injected malware into two peer-to-peer file-sharing websites,'* resulting in *up to 11,000 personal computers that were infected by malware and recruited for the attack*<sup>80</sup>.

Pirates also pose an indirect threat to others who don't download illegal content. How? Consider spam. If someone gets their PC infected with a virus that virus could be used to send large amounts of spam email to everyone in the infected users address book, including people that don't even download illegal content. The spam could include attachments that are viruses. One instance involved spammers sending out mass untargeted emails to millions of email addresses claiming that they have been logged as using BitTorrent, they even went so far as to attach 'evidence' which is actually a virus. If a user downloads/executes the attachment they would become infected. In most cases the email is designed to look legitimate, the average user would think it to be a real email from a real company not a spammer/hacker "the e-mail looks like it comes from Los Angeles-based MediaDefender ... the Hollywood ... company that is hired to fight online piracy by harassing and suing heavy downloaders/uploaders of copyrighted content." If a novice user that doesn't know any better who doesn't download illegal content gets one of these emails the might be worried and want to check out the 'evidence' thus infecting their system. The hacker successfully infiltrates another system and the poor unsuspecting users system is compromised.

Sony have also been hacked numerous times in a short time span. Lets assume for a minute, for arguments sake, that hackers used a bot net made up of hundreds of thousands of infected computers. Lets also assume that a number of these computers infected in the bot net have been infected because the users have downloaded and installed illegal software or games that have opened up their system to receive commands for use in a bot net. These computers that have been infected have now been used to hack into Sonys web serves and criminals have made off with personal details like names, addresses, user names, passwords, and credit card details of millions of people who may not even own a PC or even downloaded or used an illegal game or software title in their entire life. They through no fault of their own are being indirectly affected by those who pirate games, software, movies ect... They are, unfortunately, just collateral damage.

I used to work for an ISP and can tell you first hand that spam is a massive issue. Our users used to get their email accounts locked because they got hijacked by hackers who used the hijacked accounts to send out large amounts of spam. One email address to a spammer is useless because ISPs and many mail providers only let a user send a message to a limited number of users at once. So they hijack as many email accounts as they can to send out massive amounts of spam. But how did the users get their email accounts hijacked in the first place? Crafty spammers and hackers used phishing attacks/scams against users by sending what looked like a legitimate email from the said ISP stating that they were running maintenance on the system and to submit their user name and password so their email address wouldn't be deleted. The average user has no idea that they would never be asked for their password, ergo they think the message is legitimate and submit their user name and password to later find out that their account is locked due to spamming. So they would have to call technical support to have the issue resolved.

A virus could also possibly allow the infected machine to be used as a zombie machine in a bot net, a network of hundreds or thousands or even hundreds of thousands of zombie PCs, that is used to launch an attack against another system. Spam is usually one gateway to malware.

Being caught and getting infected with a potentially damaging virus are not the only problems with downloading illegal content. Piracy can cost users a lot of money. Take for example a user who pirates software and gets their PC infected because they downloaded some software that was infected. A user may not know that their system is being used for nefarious purposes until it gets so infested with viruses, trojans, and other malware that the system starts running slowly or doing weird things prompting them to take it to get fixed by a computer technician which could and usually does cost the user a lot to get their PC fixed. The cost to have the damaged PC repaired could possibly be more than the cost of the software they pirated that caused the infection in the first place, often negating any savings from having acquired the software legally in

the first place. E.g. A user downloads a piece of software that would cost them \$25 to buy legitimately. But they don't want to pay the \$25 so they download the software illegally, but the software contains a virus which causes their PC to slow down dramatically and do weird things. So they have a computer technician fix their PC, but the computer technician charges \$55 an hour to fix the problem, and it takes the technician 2 hours to fix the PC. All up it cost the user \$110 to have a problem fixed. The user could have saved \$85 by purchasing the software legitimately. So ultimately it cost \$85 to save \$25.

Wireless networks, more specifically unsecured or inadequately secured networks, also pose a threat to innocent users. Wireless networks can be, and are and relatively easily, hacked/hijacked. A pirate could hack/hijack someone's inadequately secured network and use it to download illegal content without the victim even noticing until they get slowed down for exceeding their download limit or worse receive a huge bill for excess data usage if they are unfortunate enough to be billed for excess usage. Even worse the user could even be locked out of their own network if the hacker manages to hack their modem/router, all it takes is for a modem to be using a default password and for that default password to be changed by a hacker then they change the modem settings to disallow any other PC except theirs to connect. The hacker then could use that connection for any number of illegal things like piracy, launching an attack, sending spam ect... And the hacker would most likely never be caught because if someone does realise and alert someone like the police the police are going to go to the ISP who is then going to go to the end user and accuse them of a crime they never committed because unknown to them someone else was using their connection for illegal purposes.

There are other risks too, less dangerous and expensive ones, risks that are merely annoying like downloading corrupt data that renders whatever was downloaded useless. Or downloading a game, a program, music, DVD or TV show only to find out it's not what you thought it was because it was labled incorrectly. Music, DVD & TV rips can be corrupt, encoded incorrectly which can cause issues such as bad video/audio quality, audio can be out of sync, the video could be partially corrupted causing artefacts, or it may not play at all, or it could just be bad quality in general. While it's not dangerous it is annoying because if you have a download limit then it means that you have just wasted some of your data allowance (and money as you are paying for that download allowance) and have to either re download, find it elsewhere to download a hopefully working copy of what ever it was that you got that was dodgy, give up or buy it legitimately.

### **Organised crime**

Piracy & counterfeiting also supports organised crime<sup>15</sup>. Organised crime gangs use piracy & software counterfeiting to raise funds for other crimes, like weapons and narcotics trafficking, contract killings ect... The low (financial and technical) barriers to starting a piracy 'business', that will return high profits combined with the low cost, minimal risk and high demand makes piracy very attractive revenue option to organised crime gangs. *A blank optical disc costs as little as 20 cents in the United States (and is free if it is stolen)*<sup>16</sup>, while counterfeit software burned to that cheap or stolen CD/DVD *"can sell for many times that amount, from 35 baht (about \$1 at 2008 exchange rates) from vendors in Bangkok, to \$5 in the streets of New York's Chinatown, or as much as \$18 if the counterfeit is passed off as a legal copy*<sup>16</sup>. It's easier than trafficking drugs and attracts less attention. *"...one kilo of pirate[ed] CDs is worth more in the EU than a kilo of pot". Generally, customs officials consider that a kilo of CDs is worth €3,000 compared with €1,000 for a kilo of cannabis resin. For instance, illicit copies of software programs, particularly for business, can generate a profit of 900%. From the economic viewpoint, the calculation is relatively simple: a computer game reproduced thousands of times costs €0.20 per copy and sells at about €45. Cannabis costs €1.52 per gram on the market and sells at about €12.29 It follows that it is eight times more profitable to traffic in digital products than drugs.*<sup>17</sup>

In September 2005 several members of New Yorks Yi Ging Chinatown Gang wre charged with 21 offences including assault, extortion, conspiracy, extortionate debt collection, witness tampering, money laundering, gambling, drug trafficking, and trafficking in counterfeit DVDs and Cds<sup>18</sup>.

The Camorra, a federation of 20 active Mafia clans, is believed to have more than 8,000 "made members" belonging to more than 100 crime families, and more than 120,000 foot soldiers, associates, and sympathizers<sup>19</sup> this is an organized-crime network based in Italy with a large international reach. They not only counterfit DVDs they also traffic narcotics, arms, human trafficking, refuse disposal, cigarette smuggling, extortion, prostitution, and loan-sharking.

May 2001, Taiwan - A raid on residential premises in Kaoshung City, located 70,000 suspected pirate discs and illegal firearms. Further searches, at linked premises, uncovered an arms factory running alongside a sophisticated CDR facility. In total 17 rifle barrels, seven modified handgun barrels, 10 shotgun barrels, 10 cartridge magazines, 50 bullets and other equipment were seized<sup>20</sup>.

Criminal organisations also use funds from piracy to bribe authorities to create safe havens where crime can flourish. Piracy is only one of many streams of revenue for organised crime gangs who use the revenue to fund other crimes often more serious crimes.

Of all the consequences of piracy organised crime and security are the two worst consequences piracy has on society and are the two biggest reasons why piracy should be reduced as much as possible.

## What is being done to stop piracy? Will it work?

The big players in the entertainment industry, RIAA, MPAA and others smaller businesses LIKE ACS:Law have tried using the law to crack down on piracy and force pirates to stop by suing individuals for their own profits and gains. This is never going to work and is flawed in a number of ways:

- 1) It's a waste of money to sue a suspected copyright infringer individually on a case by case basis, or even in a class action law suit. Millions of people infringe copyright. If you consider how much each court case costs, how many people that would have to be sued, the time each case takes. Then you have to recover the money. It quickly becomes apparent that using current laws to sue pirates out of existence thus stopping piracy is logistically impossible.
- 2) Methods used to identify pirates are flawed and are assumed guilty until proven innocent. False positives can result in innocent people<sup>21,22</sup> and even devices (anything that has an IP address like a network printer, wireless access point, even fridges that are connected to the internet) possibly being issued with copyright infringement notices<sup>23</sup>.

A lot of people think that they are anonymous on the internet but they are not 100% anonymous, it is possible to be tracked down but there is still the possibility that the end user that committed the crime wont be able to be identified. An ISP can tie an IP address to a user account, although that only identifies who the account holder is not who downloaded what. If that account holder is accused of infringing copyright for example it doesn't identify the person who committed the crime if there is more than one person at the address it could be any one or more of the people at that address that have infringed copyright, also it's possible that that account holder has an open or hacked wireless network that was used by an outsider to commit the crime.

Even Google has been served with dozens of copyright infringement warnings and has been threatened with disconnection, part of a letter sent to Google reads: *"Copyright infringement also violates your ISP's terms of service and could lead to limitation or suspension of your Internet service. You should take immediate action to prevent your Internet account from being used for illegal activities,"*<sup>81</sup>, although that would never happen. The infringement letters are designed into scaring people, scaring hem just enough, to make them stop downloading illegally.

Movie makers have even tried with class action law suits. Like makers of 'The Expendables' who are trying to sue 6,500 BitTorrent users<sup>82</sup>. Makers of Hurt Locker tried to sue nearly 10,000 people but the case was dropped<sup>83</sup>. Far Cry makers have also brought a case against 4577 users but it has had a major set back after *District Court Judge Rosemary Collyer ordered the copyright holder of the film, represented by the US Copyright Group, to limit their case only to those defendants there the Court had jurisdiction over*<sup>84</sup>. In 2010 an adult movie producer filed suit against 670 individuals who it claimed had infringed copyright on an obscure title. Now the entire case, which was presented by lawyer Evan Stone, has been dismissed<sup>85</sup>. And there are plenty of other similar cases.

So with so many cases being dismissed why are these cases still being brought to the courts? Because law firms stand to make a profit from piracy firms like the UK the ACS:Law firm, owned by Andrew Crossley, who had clients that paid ACS:Law to write copyright infringement letters to individuals. Andrew Crossley and his ACS:Law firm couldn't handle the pressure and has since quit chasing file sharers due to pressure by courts. Even RIAA and MPAA (and others) have admitted that suing is not the answer, *"The role of lawsuits in solving the online theft problem is clearly limited,"* wrote the coalition that included the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA)<sup>54</sup>.

With law suites failing corporations are looking at other ways of stopping copyright infringement. The RIAA and other corporations has turned to lobbying/suing for ISPs to police it's own users. In 2008 AFCAT (Australian Federation Against Copyright Theft) represented Village Roadshow, Universal Pictures, Warner Bros Entertainment, Paramount Pictures, Sony Pictures Entertainment, Twentieth Century Fox Film Corporation, Disney Enterprises, Inc. and the Seven Network in a court case against Australian ISP iiNet. AFACT claimed that an ISP should be responsible for it's users actions. However Judge Justice Dennis Cowdroy ruled against AFACT. iiNet won the case, but AFACT appealed the case and iiNet went back to court and won a second time. In the wake of the second ruling the Internet Industry Association announced that it will begin work immediately on a code of conduct for the ISP industry. iiNet has also released a white

paper that suggests copyright infringers should be treated like speeding drivers, with demerit points and fines issued to copyright infringers through an independent mediator funded by copyright holders. Whether this will work or not is yet to be seen.

Ultimately suing was never going to work because the sheer numbers involved and the bottom line is that major corporations (namely the music and movie industries) are trying to force an old business model to work with a new digital economy. The old business model is never going to work with a new digital economy. Corporations need to re model their business plans to work in a new digital economy. The internet, broadband, along with the power and cost of computers and more specifically the cost of storage has given birth to a a digital economy that calls for new types of business models.

The gaming industry struggles with the issue of piracy but it is actively doing something about piracy by developing business modes that work in a digital age. Steam is a perfect example. It makes it quick, easy and convenient to buy games and the games are relatively cheap. Steam also has built in anti piracy measures. Steam has in one example seen sales of a particular game, Garry's Mod (or more accurately a tool for a game (Half Life 2)), jump by 1074%<sup>40</sup>.

Some parts of the music industry have also gone digital, there are over *500 legal music services worldwide*<sup>35</sup> like iTunes, Beat Port, and Juno. Digital music sales are coming close to that of CD sales "digital music sales [are] growing at 15 to 20 per cent, and CDs [are] falling by an equal proportion, digital music sales will nearly equal CD sales by the end of 2010."<sup>36</sup>, "Paid digital music downloads accounted for 35 per cent of all music sales in the first six months of the year, up from 20 per cent in 2007 and 30 per cent last year."<sup>37</sup>, and "iTunes accounts for 25 per cent of all music units sold, up from 14 per cent in 2007 and 21 per cent in 2008"<sup>38</sup>.

### **Education**

A number of groups, including the RIAA, MPAA, BSA etc are trying to educate people that infringing copyright is wrong. They are using a number of methods including ads & web sites to spread their message. But most people that infringe copyright know that it's wrong and no amount of education will stop them.

### **DRM & Other technologies**

DRM & other technologies like Region locking / Territorial distribution are used to restrict the use of media like games, movies, music, etc. This has a limited effect as DRM & other copy protection technologies can be, and often are, reverse engineered and bypassed.

### **Law reform**

Copyright laws are so old and out of date that they need to be reformed to apply to a digital age. It is getting increasingly harder to apply old laws to new problems that are coming about because of computers and the internet. Copyright law may have been useful in the world pre computers and sans internet in a world where books were the ultimate source of information. But that time has long since passed and has given way to the digital age.

There are political parties around the world like the Sweedish Pirate Party & Pirate Party Australia who are fighting for copyright reform and other issues like civil liberties.

Founded in 2001 by founded in 2001 by Larry Lessig, Hal Abelson, and Eric Eldred Creative Commons have "*released several copyright-licenses known as Creative Commons licenses. These licenses allow creators to communicate which rights they reserve, and which rights they waive for the benefit of recipients or other creators*"<sup>41</sup>. Creative Commons "*seeks to support the building of a richer public domain by providing an alternative to the automatic "all rights reserved" copyright*"<sup>42</sup>. There will always be a place for traditional copyright but it's importance will diminish. Already the Creative Commons licence has been upheld in a Belgian court of law *when a band called Lichôdmapwa won a lawsuit against a theater company in Brussels*<sup>50</sup>. Governments are adopting the Creative Commons like Australias Bureau of Meteorology<sup>51</sup>, DBCDE<sup>52</sup> and there are plenty of other examples in over 300 case studies<sup>53</sup>.

## **What else can be done?**

The problem is that anything that is or can be digitalised can be pirated. So if we accept that copyright infringement will never be stopped 100% then what else can be done? To slow down piracy every method used for piracy needs to be addressed since piracy affects more than the software, game, movie and music industries.

## **Education**

One thing that can and is already being done to combat copyright infringement is education. Some people know it's wrong but still do it, others are blissfully unaware that what they are doing is wrong. There is more that can be done to combat piracy other than just making people aware that piracy is wrong, education should also include making people aware of the alternatives like free open source software (FOSS) alternatives to expensive software like Microsoft Office, Adobe Photoshop etc... FOSS is growing in popularity and is often just as good, if not better in some cases, than commercial paid for versions of games and applications.

For the average person who just uses their computer to surf the internet and email there is no reason why they should pay more, beyond the cost of the hardware, for their computer. Using a Linux Operating System (OS), and Free or Free Open Source Software (FOSS) for things like web browsing Firefox or Opera are even better than Internet Explorer, if it's word processing or making spreadsheets Libre Office is a free alternative, backing up data can be done for free with Macrium Reflect, Thunderbird can replace Outlook ect... There is usually a FOSS alternative to most programs any average user would ever want to use. The problem is that it's not known or that there are misconceptions that FOSS is not as good because it's free. People in the know should be taking it upon themselves to educate those who know no better.

For TV and film there are alternatives like YouTube and Vimeo where producers of TV and film post videos. Take The peoples Republic of Animation<sup>26</sup> for example who have posted their productions (like The Ghastly Gourmet Cooking Show) that have been aired on commercial TV but have been posted to free video streaming sites like Vimeo. Then there are podcasts like <http://www.channelfrederator.com/> that offer free podcasts. Shows like Good Game<sup>27</sup> that offer downloads that can be viewed on portable media players (PMP), then there are 'catch up' services like ABC's iView<sup>28</sup> that offer full length TV shows on demand.

For music there are alternatives like Jamendo that offers free music from thousands of artists across hundreds of genres, all licensed under the creative commons licence.

Education alone is not enough to stop copyright infringement, I don't think the new version of "Don't copy that floppy" is going to cut the mustard... It's all about the internet these days and even CD-Rs are getting old. People are more likely to listen to their peers than they are to a half arsed video about not copying that obsolete media that is not used any more. Although education can do a great deal of good there are other ways of combating copyright infringement that when combined with education can make an even bigger difference in fighting any type of copyright infringement.

Addressing the reasons why and methods that people pirate is another, often harder, way to curb piracy.

## **Internet piracy**

Internet copyright infringement is the biggest and hardest problem to solve given the availability and uptake of DSL and other super fast broadband connections and the price & performance of computers and internet connections plus there is any number of ways that people can infringe copyright on the internet from using programs like BitTorrent, or downloading from FTP sites, from file servers, to direct downloads from web pages to using copyrighted material on web sites. To tackle internet piracy there are a number of issues that need to be addressed;

Convenience. People pirate because its convenient. It's 12:00 midnight and the shops are shut so you can't go to the shops and purchase the game/application/music/movie ect... that you want. This is where Digital downloads can make a huge difference by making content available 24/7. The only potential problem that may need to be addressed is that of ISP metering the content, a customer pays for the content then they download it then the data is counted towards their download limit that they pay for so they have effectively been charged 2x for the download. Compared to illegally downloading the content for free, the data is still counted towards their download limit but they are only paying once since they only pay for access and bandwidth/a download limit. Not every ISP as unlimited plans. If ISPs didn't meter digitally downloaded content from select digital distributors then downloading legal content would possibly become much more attractive.

Removing DRM, do away with regions/territorial distribution, offering better value for money and or lowering the cost, doing away with use by dates, offer previews/demos, and making it easy and convenient for users to get what they want when they want can go a good way towards reducing internet piracy.

There are also some other unorthodox ways that publishers are combating piracy like intentionally leaking a

new game that is in development, but leaking it on purpose with bugs in it. Like the PC version of Batman: Arkham Asylum which prior to being officially released was intentionally released with glitches that make the game impossible to complete<sup>33</sup>. However this was only a temporary solution as the glitch was soon fixed by crafty coders. It is a good idea that could be developed further to combat game piracy.

Valve's founder Gabe Newell has a novel idea whereby the community invests in the game, "Right now, what typically happens is you have this budget - it needs to be huge, it has to be \$10m - \$30m, and it has to be all available at the beginning of the project. There's a huge amount of risk associated with those dollars and decisions have to be incredibly conservative,"<sup>35</sup> said Newell.

"What I think would be much better would be if the community could finance the games. In other words, 'Hey, I really like this idea you have. I'll be an early investor in that and, as a result, at a later point I may make a return on that product, but I'll also get a copy of that game.'" <sup>35</sup>

Film makers are already doing what Gabe Newell is talking about. A project by the Riot Cinema Collective have asked people for donations to help them finish their film 'The Cosmonaut' after a backer of the film reduced their contribution or backed out. People contributed, they raised the funds they needed and work is continuing on the film.

There are start-up fund projects specifically for games, "*Indie Fund is a funding source for independent developers, created by a group of successful indies looking to encourage the next wave of game developers. It was established as a serious alternative to the traditional publisher funding model.*" their aim is to "support the growth of games as a medium by helping indie developers get (and stay) financially independent."

A web site called Kickstarter is helping people fund projects by letting people contribute money to projects (Art, Comics, Dance, Design, Fashion, Film & Video, Food, Games, Music, Photography, Technology, Theater, Writing & Publishing) in return for a gift or gifts. Projects are posted with a monetary goal and a time frame in which to reach that goal. People can choose how much they want to pledge. If the project reaches it's goal within the time frame then the money is donated, if the goal is not reached before time expires then money doesn't change hands. Kickstarter describe it as All-or-nothing funding which means "it's less risk for everyone. If you need \$5,000, it's tough having \$2,000 and a bunch of people expecting you to complete a \$5,000 project".

Makers of 'The Tunnel' are trying a novel approach by releasing the film for free on bittorrent but also selling frames to the film as well as the DVD that has additional content like alternative endings. On the film web site they reason that:

*The Internet was meant to be a tool to connect us. It was meant to break down borders and liberate. Now we have an entire generation who are being labelled criminals for using that tool. But perhaps rather than wasting millions of dollars fighting a losing battle against internet piracy, we should try and find a way to embrace the possibilities that this new world brings...*

*That's the thought that inspired this project. We believe that if we stop fighting the peer to peer networks, they could become the biggest revolution we have ever seen in the way we share entertainment and information.*

*After spending years being frustrated by what we saw as the movie industry's short-sighted and conventional outlook towards the online community, we decided it was time to try something different - The 135K Project was born.*

*We figured that movie posters and collectable frames from movies are being sold every day, so what if we could raise the money to make "The Tunnel" by selling every individual frame of it? We would be able to make a movie unencumbered by a studio's need for box office. We could do what we got into the industry to do in the first place. Tell stories we like and get them out there so people could enjoy them.*

*What's the key to doing that? You.*

*If you like the look of "The Tunnel" or the idea behind The 135K Project - buy a frame or two, blog about it, follow us on twitter, seed and embed the finished film when it's released. Whatever you can do. It will all help and show the world there might just be another way. Who knows where that might lead?*

There is nothing stopping larger corporations and developers implementing the afore mentioned ideas to

help fund their projects.

### ***OEM unbundling***

Again people use OEM unbundling as a way of profiting from piracy. And trying to make it unprofitable in the first place is going to be the best, but also the hardest, way to stop this type of copyright infringement. A more immediate solution would be the report and bust method. Education is another tool that can be used. OEM unbundling shares the same problems as software counterfeiting does. One solution could be to include no software on CD (apart from the necessary driver software required to get the hardware working and hardware manual) with hardware and make the programs downloadable and only include a link with a user name and password (via email) upon registration of the hardware then the user goes to a page and uses the user name and password to get access to the OEM software directly from the manufacturer. If the customer doesn't have an internet connection they could mail-order or phone to ask for the software to be sent out. If users have to actively do something to get the software they are less likely to try and sell it because they won't be able to if they have to download the software, there is no CD to sell. It makes it harder for the pirates to resell OEM software. It could also be made traceable so if someone did sell or try to sell the software it could be tracked.

### ***Hard disk loading***

It's close to impossible to stop people from installing illegal content on to computers, so education is going to be the next best way to combat this type of copyright infringement.

Purchasing a PC with illegal software installed on it makes it a lot more expensive to repair. As a computer technician I often have to reinstall someone's operating system on their PC, for example if they get a virus then I will reinstall the OS since it's the only way guaranteed to get rid of the virus. If the person has an illegitimate copy of an operating system then I will not install it, I have had customers bring illegal copies of Windows for me to install which I refuse to do. I will tell them that what they have is illegal and they will have to purchase a legitimate copy of the software.

If people know what to look for when they are buying a PC and know what questions to ask they can avoid purchasing a PC with illegal software on it. They will then be able to make a better decision whether or not they should purchase a PC from the particular seller. If they know that a PC has illegal software installed on it and still choose to buy it then that is their decision, one that could cost them later if they need to have the PC repaired. There are always going to be people who will only look at the initial price and not give a second thought to the potential cost of maintaining the PC or any other potential extra costs that may arise later on.

Consider someone that has a PC who chooses to pirate a \$25 piece of software. To illustrate my point let's say the illegal piece of software that they download has a virus, they install the piece of software and it infects their system and causes the system to come to a grinding halt and the system takes 10x longer to do anything. Just turning on their PC takes 10 minutes before it can be used and even then it feels slow once it has finished booting. They have no idea what is going on and they don't have enough knowledge \*which is proven by the fact they illegally downloaded the software in the first place) to fix the problem so they take it to a PC technician who charges them \$110 to fix the problem. That user probably won't install that piece of software again, and they are an extra \$110 out of pocket. All up it cost them \$135 because they didn't want to pay \$25 for a piece of software.

It's the same when purchasing a PC. Someone might be able to purchase PC A for \$950 or PC B for \$1225. PC A is cheaper because the builder installed an illegal copy of Windows on it and doesn't provide the customer a copy of the Windows disk. This person chooses to buy PC A because it's cheaper, regardless of whether or not they know why it's cheaper. Later on they have a blackout while using the computer, they try to turn the PC on after the black out but the PC won't boot into windows. It gives them some blue screen with white writing on it saying something about a fatal error. So they get a computer technician to have a look at the PC who advises them that the operating system needs to be installed and asks them for the Windows disk they got with the PC, the customer says they never got a Windows disk. The technician then informs them that they had an illegitimate copy of windows on their system and that on top of the technicians fee of \$165 they will have to purchase a legitimate copy of windows which costs \$259 before their PC can be repaired. The customer goes and purchases a copy of windows, the technician completes the work and \$424 later the customer has a working computer again. If the customer had purchased the PC that cost \$1225 that came with the legitimate copy of Windows pre installed along with the Windows disk should they ever need to install their operating system they would have come out \$149 richer because they would have only had to pay the technicians fee of \$165 to fix the PC rather than an additional \$259 for a legitimate copy of Windows.

Give people the knowledge and let them decide what to do with that knowledge. If someone knows that purchasing a cheaper PC that has illegal software installed on it could cost them more later on but still

chooses to make the purchase because it is cheaper than the legitimate option then that is their decision. They can not complain (although they still will piss and moan about it) if their bad decision comes back to bite them. Most people would make the right decision if they know that choosing the cheaper option could cost them more later on.

### **Renting**

The rental market isn't as strong as it was and brick and mortar rental shops will maybe one day die when online purchases or rentals become the normal way to buy or hire a DVD. But to deliver rentals over the internet there needs to be in place a high speed internet connection/network to deliver the content. It is fairly easy to put time limits on downloads so if a user doesn't download/watch the movie in a given amount of time the content will expire and the user will no longer have access to it. Streaming content could also possibly make it harder to copy, to the point that it becomes too impractical and not worth while copying the content. There is no reason technologically why delivering content over a network, i.e. the internet, can not be done right now. It's people and corporations with vested interests in profiting by keeping content under lock and key that is holding back the future. The future is already here — it's just not very evenly distributed. - William Gibson in "The Science in Science Fiction" on Talk of the Nation, NPR (30 November 1999, time stamp 11:55)

### **Cracking/Patching/Keygens**

Cracks, patching and keygens (serial key generators) work by upgrading a trial or shareware version of a program to the full version or by unlocking features that are otherwise unavailable or that stop a program from working after X days without the user having to pay for the serial key. One problem is that a lot of key gens, cracks and patches contain a virus in the software that is used to crack or patch a program or generate a serial key. Educating people about the dangers of using such methods to obtain fully working software is one tool that can be used to combat this type of copyright infringement.

The other half of the problem is that coders code programs with these features built in that are simply locked and are ununlockable via a purchased serial key. This could be avoided if coders only offered a cut down version of the program that was only valid for 30 days, upon expiry of the program they would have to purchase the full version of the program via some sort of digital distribution platform.

### **Softlifting**

Software as a Service (SaaS) could be a possible solution to some types of software piracy. Games like WoW & Eve online where players pay a subscription to play are a good point in case, you can have the client (the software) for free but without access to the servers to play the game the software has little to no use at all. Software like CRM applications like Sales Force have also used SaaS effectively.

Another possible solution is to offer the software for free and have paid support. Offer a free unsupported version (as opposed to a shareware or trial version that expires in X days or that only has limited functionality) of an application with fewer features and offer a full version, a paid version with a full features list and full support.

In addition the Software & Information Industry Association (SIIA) have a system whereby piracy can be reported and if a report leads to a successful settlement and rewards of up to \$1,000,000 can be given but this only applies to "*cases of corporate end-user piracy*"<sup>30</sup> so there is not much incentive for people to report general piracy like casual or internet pracy. Maybe smaller rewards can be offered to people for the successful conviction for selling of counterfeit software, weather it be via the internet or at computer swap-meets, markets, ect...

### **Miscelanious**

Copyright can be infringed in any other number of ways like internal leaks/lack of security - It is entirely possible that an insider can leak content. This is an internal issue that content developers need to address. It's possible that hackers can hack into a system that is being used to develop and hold content that is being developed. Again this is an internal security issue that needs to be addressed.

Then there are those who do it because they can, because they can. People who reverse engineer software and systems shouldn't be looked upon as criminals. They have a valuable skill that and they should be encouraged to use their skills for the good of society. Rather than punishing these people, companies and corporations should be hiring them as security testers.

So I have addressed how to reduce piracy by addressing the way people pirate but a more important issue to address is why people pirate. If the issue of why can be addressed then how people pirate becomes less relevant.

### **Stop treating customers like criminals**

All DRM and restrictive licences do is treat customers like criminals and make them more likely to pirate content rather than have to deal with cumbersome DRM. Take audio books for example, Audible like to release audio books in their own propitiatory format that can only be played on some devices. Why not just release the books in an MP3 format rather than releasing audio books in a propitiatory format and restricting the devices that the content can be played on and forcing customers to illegally download or convert the content into MP3 format. There needs to be trust that users will do the right thing. Would you buy something then just give it away to some stranger for free?

Don't even bother with DRM. DRM causes more issues than it solves and usually pushes people to download illegally or just boycott anything that is DRM'ed, either way sales are missed out on. Using DRM on products is the equivalent of treating people like criminals. It is saying that we do not trust you so we are going to assume you will infringe the copyright, our intellectual property, of our product ergo we are going to enforce DRM on you. One of the reasons why people download illegal software, music, films ect... is so that they don't have to deal with DRM. People want to own what they buy and be able to use it how they want. Why would you buy an mp3 online if you can only listen to it on one brand of PMP?

### ***Because they can***

There is not much you can do about people prating because they can. There isn't much that is going to stop people pirating because they can. If they can they will. Just because they can and do doesn't mean they watch, use, play, read whatever they pirated so it's not necessarily a lost sale.

### ***Because it's not available any more***

There is no reason in the digital age when a digital product should no longer be available for purchase. Granted that DVDs cost money to produce & ship to retailers. Rather than just ceasing production of a product, after it's artificial use by date, should be made available online. It costs a lot less to distribute a product digitally online than it does to make the physical product. I would argue that the product should be made available online instead of packaging it and transporting it for sale as it would not only save the producer money. Digital distribution will also save the environment since the data is transferred over cables and consumes less of the earths resources for packaging and transportation because there is no packaging and transporting data over the internet is a lot faster and efficient. Steam is a great example and cold be done with any type of content like music, movies, software, books ect... And it's only just starting to happen but the problem is that the content is locked up in proprietary formats and DRM.

### ***For profit***

People counterfeit software for profit, the challenge is to make counterfeiting unprofitable but making it unprofitable is the hard part. People can report counterfeited software and the people involved can be fined/imprisoned thus making it unprofitable for them but then there is always someone else doing it that has yet to be caught. Software counterfeiting needs to be unprofitable from the start so that there is no reason to counterfeit software in the first place. Education and having people report counterfeit software is one method in use today but this can only curb counterfeiting to a certain extent as only known counterfeiting can be stopped. The problem is that people generally find it hard to tell the difference between the fake and the genuine article making it harder to report counterfeited software if they wanted to. Education can help, but only if people take notice. Mostly people are just happy that they got what they think is a bargain and wouldn't think twice about it. Counterfeits are sold at markets, computer swap meets and online via web sites and spam emails. Software counterfeiting is best stopped before it is sold to unsuspecting consumers. The problem is that counterfeit software is distributed physically in a number of different ways which makes it hard to police. I would suggest targeting the markets and web sites where counterfeit software is sold. The average Joe, the kid that sells the odd copy at school to school mates isn't a major criminal and isn't making vast amounts of money to fund other criminal acts ergo they should not be the target of policing. But at the same time it should not be ignored, but just not policed as heavily. The root cause of the issue needs to be addressed not just the symptoms, prevention is better than a cure.

### ***Region locking / Teritorial distribution***

Get rid of it altogether. Why sell only to 306,617,000<sup>25</sup> people (4.52%<sup>25</sup> of the worlds population) when you could sell to 6,785,100,000<sup>25</sup> people? If you sell to a potential 306,617,000<sup>25</sup> people, and you only sell 1,000,000 units @ \$25 then that is \$25,000,000. If you sell to a potential 6,785,100,000<sup>25</sup> people, and only 1,250,000 buy @ \$25 that is \$31,250,000 or more than you might have otherwise made.

Now imagine that only 1,000,000 out of a potential 306,617,000<sup>25</sup> purchase a unit of your product because you only sell it in America, how many of those 6,785,100,000<sup>25</sup> potential customers want a unit of what you were selling @ \$25 and are willing to pay for it but are unable to get it? Lets say the said unit is series 1 of a popular TV show, it only takes 1 person to upload a copy to the internet (assuming there is no DRM or that the DRM has been cracked) to make it available to millions of others who will download it for free.

Sure people are still going to download your product for free if they can. But how many people that download

your product, for free, were actually willing to pay for it in the first place but pirated it because they couldn't legally buy your product?

If, for example, a DVD is released in region 1 first then released in the other regions a month apart then some one is bound to rip the DVD and post it online for download. How many people are looking forward to that release so much that they will download an illegal version just so they get to see it because they don't want to have to wait? If a DVD is released in every region at the same time then people would be less inclined to download the ripped version of the said DVD title because they are able to buy it legitimately from the shops instead of having to wait.

### **No demo/trial version**

This is a no brainer, release a demo. Even if it is only the first few levels of a game, or a trial of an application, preview of a song or movie a trial/demo should be released. People often state that they pirate a game or application because there is no demo. If these people had access to a demo then they wouldn't need to pirate the software just to try it. Once the software is pirated and the user decides they like it they are less likely to purchase a licence to use the software because they already have the full version that they pirated, although some people will still purchase the software legitimately.

### **General errors, quality & pricing**

Make the product better quality, if it's not better quality then lower the price, people will put up with something of lesser quality if its cheaper. But what constitutes quality? For games it's price vs. content, how many hours of entertainment will it offer, is it replayable? Multi player games offer unlimited replayability as everytime you play the game it will be different. For software it's features and ease of use. For music and movies it's sound and picture quality.

Why sell something at \$100 if only 5 people can afford it? Why not lower the price to \$50 then more people can afford your product, and the more chance you have of making a larger profit. The lower the price the more people can afford it and the more likely they are to purchase it on impulse. *75% of survey respondents indicated that a "special sale price" would motivate them to make a spontaneous purchase.*<sup>29</sup>

If someone wants 2 movies that cost \$30 each but can only afford 1 then they purchase the movie they want and go without the other movie, maybe indefinitely (they might forget about it or decide they don't want it by the time they can afford it or they might just pirate it instead) or they will purchase it at a later date, or purchase it when it's on sale for say \$10. If those 2 same movies cost \$15 each and could be downloaded straight away using digital distribution then the customer is probably more likely to buy both movies because they are cheaper than the 1 physical copy of a movie.

### **For the challenge**

Instead of cracking down on crackers companies should be hiring these people to help them improve their security. Reward instead of punishing people that are smart enough to defeat copy protection and other copyright schemes.

## **Piracy as part of the eco system**

In nature fires, floods, hurricanes, earthquakes and all sorts of natural disasters are commonly thought to be a bad thing. Natural disasters are not always a bad thing, take fires for example, the only way some plants seed pods will open and drop their seeds for germination is if they are scorched by fire. Fire is bad if it's in a house or in a built up population or if it's deliberately lit but it can also be a good thing that can renew and regenerate life if it happens naturally. Piracy is similar to a fire, it's commonly thought to be bad but it has its place in the economy. There are plenty of third parties that benefit from piracy, and even the industries that cry foul over piracy benefit from it oddly enough.

Take the tv/movie and music industry for example. They not only produce tv/movies and music they also collect licence fees from third parties who make and produce merchandise to sell along side tv shows, movies and music. Merchandise like apparel (think band t-shirts), posters, action figures, collectables, vinyl toys, trading cards ect... In 2010 the United States Government Accountability Office did a study called INTELLECTUAL PROPERTY: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods they found "companies may experience increased revenues due to the sales of merchandise that are based on movie characters whose popularity is enhanced by sales of pirated movies."<sup>87</sup>, piracy is essentially free publicity.

The music industry is one of the most vocal opponents of piracy yet piracy can help by providing helpful

insights into a music fans interests. In 2008 the Economist ran a story called *Thanks, me hearties* that highlighted how piracy data is helping the record industry; the articles writer was of the opinion that “Such information can help managers promote their artists. Jennifer Bird of Red Light Management, a management agency in Los Angeles, says her agency knows the names and geographic destinations of the 7.5 billion songs swapped in 2007. That is a big help if you are trying to work out whether people are raving about an artist—or merely about a song. And planning joint tours is easier when you know what other music an artist’s fans listen to.”<sup>88</sup>. BigChampagne, a firm based in Beverly Hills, California, that compiles and sells statistics about file-sharing started monitoring the file sharing of “television programmes and films, which are also widely shared online. Knowing what is popular among file-sharers could help broadcasters and film studios when negotiating with advertisers, for example. Hulu, a website operated by News Corporation that offers free, advertising-supported video-streaming, already uses file-sharing statistics to design its programming and to set advertising rates.”<sup>88</sup>.

In another Economist article the writer states that “Statistics about the traffic on file-sharing networks can be useful. They can reveal, for example, the countries where a new singer is most popular, even before his album has been released there.”<sup>89</sup>. The same article also highlights the fact that *In other industries, piracy can help to open up new markets. Take software, for instance. Microsoft’s Windows operating system is used on 90% of PCs in China, but most copies are pirated. Officially, the software giant has taken a firm line against piracy. But unofficially, it admits that tolerating piracy of its products has given it huge market share and will boost revenues in the long term, because users stick with Microsoft’s products when they go legit. Clamping down too hard on pirates may also encourage people to switch to free, open-source alternatives. “It’s easier for our software to compete with Linux when there’s piracy than when there’s not,” Microsoft’s chairman, Bill Gates, told Fortune magazine last year.*<sup>89</sup>.

Oxford economist Karen Croxson has suggested that digital piracy “does not necessarily undermine profit as pirates may actually help to promote the product they steal”<sup>90</sup>. In a news article on the University of Oxford’s web site Ms Croxson points out that “piracy poses a threat to sales only when those who otherwise would buy become tempted instead to copy. She goes on to say that “In any market there are some who value the product but never would buy. Their piracy cannot harm the seller. Quite the opposite: because, like any consumer, a pirate will talk to others about product experiences, copying which does not displace sales can actually help business. Consumer ‘buzz’ is hugely important for sales success, studies have shown, and piracy drives up buzz without the need for extra marketing.

The article continues: *Ms Croxson’s analysis considers the temptation to copy a product illegally. This comes down to quite personal factors. Relevant parameters include the value of time, fear of penalties, and moral costs. Modelling this behaviour enables her to predict the variation across markets in the genuine threat to sales and the optimal response of the seller in different cases.*

*Computer games, for example, are protected heavily because their products are aimed at the youth market. Younger people tend to value games most, but may worry less about copying illegally and have more time on their hands. Piracy may be cheap for them, but their copying, because it undermines sales without generating extra promotional benefits, is detrimental to business. A taste for draconian anti-piracy measures, unsurprisingly, is prevalent among games manufacturers.*

*In contrast, business software producers appear to put lower effort into protecting their products against piracy, and the reasons may not be immediately obvious. The model provides some explanation. Professional users are known to attach a higher worth to office software than, for example, students. At the same time, they are likely to have higher piracy costs as their time is more precious and they may focus more on legal repercussions.*

*Ms Croxson explained: ‘With valuable users shying away from copying, the sellers in the business software market find themselves more naturally insulated against lost sales. Those more inclined to pirate, perhaps students, probably wouldn’t have bought the product anyway, so represent virtually free promotion. This helps explain why business software companies do not put as many resources into protection as computer games manufacturers.*

*‘Building a theoretical model of ‘promotional piracy’, it is possible to distinguish markets that are best advised to put considerable resource into safeguarding their products from others which may live quite comfortably with a higher incidence of digital piracy.’<sup>90</sup>.*

Internet Service Providers, or ISPs, profit directly from piracy. Pirates will want the fastest connection possible with the largest download limit they can get. The fastest plans with the largest download limits are usually the most expensive plans available. ISPs know this and make plans available that are attractive to large downloaders, like iiNets Home 4 (bundle) plan which offers ADSL2+ speeds with a 1 TB download limit,

500 GB during peak and 500 GB off peak or TPGs ADSL2+ Unlimited plan which has no limit so a pirate could download as much as they can or want. There are some people that would argue that such large download limits are only aimed at pirates, but there are legitimate uses for ultra fast plans with large download limits. Take Steam for example, all Steam games are delivered digitally over the internet and it's not uncommon for a game to be 1 or more GB in size, often games are multiple gigabytes in size like Command and Conquer Red Alert 3 for example which is 7050 MB or 7 GB, some plans don't even offer 7 GB per a month. A heavy gamer may buy quite a few games from steam, I have 49 games in my Steam game library, if I were to download all of the games I would need an allowance in excess of 50 GB. Other business like VPN (or Virtual Private Network) Service Providers are also benefiting from piracy. There are a lot of VPN providers that offer free and paid for services. As mentioned earlier users are not 100% anonymous on the internet. VPNs lets users hide their IP from the public and anyone trying to track them, it makes their internet connection anonymous, data is also encrypted so that it can not be intercepted. Piracy and privacy have become much bigger issues recently and a VPN is a good solution for making a connection anonymous and it is being marketed as such, there are any number of articles, like Torrent Freaks "5 Ways To Download Torrents Anonymously"<sup>90</sup> article, that promote VPNs as a great way to make yourself anonymous on the internet.

Software manufactures also benefit from piracy. There are plenty of software solutions that bypass copy protection security like SlySofts CloneDVD which lets a user copy a DVD. SlySoft also make AnyDVD which removes encryption (CSS), and region codes which will let a user play a DVD from any region, it also removes analogue copy protection (Macrovision) and features such as forced subtitles and warnings. The afore mentioned two software titles sell for 39 and 49 Euros each. There are plenty of other software titles that can and are used for piracy that are paid for and a lot that are free as well.

Hardware manufacturers also profit from piracy. Storage manufacturers profit the most as a direct result of piracy since all those illegal games, applications, movies and TV shows aren't small files and if movies and TV shows are recorded at 720/1080 HD quality then the files are going to be so large they are measured in gigabytes. Right now, as I write this the largest HDD you can buy is a 3 TB HDD which will set you back well over \$200, not exactly cheap. Optical disk manufactures also profit directly from Piracy as do manufacturers of Media Players like A.C.Ryan, Astone, Western Digital, Dvico. Media Player manufacturers make devices that will connect to your network and let you stream content straight to your TV, some media players let users plug in a HDD that has content on it they want to watch on their TV like movies, TV shows, music which has probably been illegally downloaded. Media player devices aim to make it as easy as possible for a user to setup and use. Media streamers also promote piracy, although the manufacturers would never admit it, by offering features like built in bittorrent clients. Manufacturers know that their devices are used to view and listen to illegally downloaded content.

The general public didn't know about digital music or what an MP3 was until personal media players came out like the iPod. All of a sudden there were these devices that could play MP3s and people discovered digital music, they also discovered they could download MP3s from the internet for free. Personal media players drove the demand for digital music and also drove music piracy rates higher because when personal media players first appeared there were no online music stores so people would resort to pirating music to listen to on their personal media players. Manufacturers of hardware like HDDs, media players and personal media players know that their users are using their devices to access and store illegal content but they are making a profit from piracy so why would they do anything about piracy? To do something about piracy would be like throwing money away.

Even computer component manufacturers have benefited from piracy thanks to the growth in popularity of Home Theatre Personal Computers or HTPCs. The true geek doesn't bother purchasing pre built media players, a true geek will build their own PC to perform specific tasks like for playing games or in the case of the HTPC watch and record TV, play movies, blu ray DVDs and listen to music. A HTPC can do everything a media player can and more. HTPCs are basically a normal PC built to be as quiet as possible (because they usually reside in a living area so they need to be quiet so they don't disturb the user while they are watching a movie) with carefully chosen parts. The movies and TV shows that are watched on the HTPC are usually ones that have been downloaded. So when a HTPC is built to watch illegal content the computer component manufacturers (like CPU, RAM, motherboard, PSU, etc...) are indirectly benefiting from piracy.

All the talk that piracy costs jobs may be true but it also makes and supports a lot of jobs as well. Think of hardware manufacturers, they need employees to run their factories, ship their goods, to market their goods. Service providers like ISPs need people to market, sell and provision their services. Where jobs and money is lost in one industry they are made in another.

It could be argued that piracy has given birth to new businesses and promotes innovation. Without piracy media players and personal media players may never have been invented, if they were invented then their development may have been a lot slower than it is today without piracy. Without piracy there would be less need for VPN services, ISPs probably wouldn't be offering plans with large download limits, software makers

wouldn't be making software titles that aid piracy. If you add up all the money that people spend on the aforementioned services that is a lot of money that flows into the economy and provides a lot of jobs. There are a lot of industries that benefit directly and indirectly from piracy, ultimately piracy is part of an eco system, part of the economy.

## Conclusion

The reasons for wanting to reduce piracy should have nothing to do with loss of revenue because it is fairly well known that revenue losses are not as bad as it is made out to be. Additionally piracy supports other industries and businesses. There are more important reasons for wanting to reducing piracy. If piracy is reduced it follows that the internet and computer systems will become a little bit more secure, although there are plenty of other factors in security that need to be addressed but that is beyond the scope of this essay. Just as importantly counterfeiting needs to be reduced as much as possible because counterfeiting can and is used by criminals to help fund other illegal activities that have far worse consequences than just loss of money or jobs.

Piracy is also committed by large businesses and corporations that see piracy as a way of cutting costs. It could be argued that Piracy is alive and well because of major record labels who are selling works that they do not own the rights to, Grace Maxwell (wife and manager of UK indie rocker Edwyn Collins) says 'Illegal' file sharers are not the problem, "[We are] aware of who the biggest bootleggers are. It's not the file sharers. [A Girl Like You is sold] not by Edwyn, [but] by all sorts of respectable major labels whose licence to sell it ran out years ago and who do not account to him."<sup>39</sup>. It turns out that major record labels have been selling music they do not have the rights to sell, which is essentially piracy. Ubisoft has also been accused, in a rather bizzare case, of piracy for *selling pirated materials which it itself made as part of the Collector's Edition of Assassin's Creed: Brotherhood. The accusation revolves around the soundtrack for the Digital Deluxe Collector's Edition of Assassin's Creed: Brotherhood, the meta-data of which reveal it to be a tormented version which was encoded by 'Arsa13', rather than Ubisoft*<sup>86</sup>.

Piracy is an issue that needs to be regulated, not stopped out at any cost. To completely eradicate piracy would kill businesses and industries and stop a lot of money flowing back into the economy. A person may choose to spend more money on a better video card to play games then pirate the games, rather than spending \$300 on a video card and \$50 on a game they instead spend \$350 on a better video card. That money is still being spent and flowing back into the economy. You can apply the same scenario to personal media players, a person might spend \$150 on a personal media player instead of \$100 on the personal media player and \$50 on music to put on the media player.

Piracy is never going to be stopped given the number of ways and reasons why people infringe copyright. The issue is too complex to for one single solution to prevail. Each reason and method of piracy needs to be addressed individually on its own with the solution depending on the reason and method of piracy. There needs to be a massive effort on many fronts to reduce piracy because the bottom line is that piracy will never be stopped and current efforts to forcibly stop piracy will fail epicly. Corporations need to stop fighting the new digital age and digital economy and embrace it and be proactive about developing new business models for a digital age instead of trying to force an old model to work in the digital world.

People and especially corporations need to look at piracy as a part of something bigger, as part of an eco system, rather than as a problem that needs to be stopped at any cost. A different perspective on piracy is needed, the whole picture needs to be taken into account rather than narrow pints of view. A new way of thinking about piracy is needed.

I don't believe that casual piracy is the problem it's made out to be. I would agree that people, businesses, corporations and anyone that that pirate for a profit (i.e. knowingly pirate for a profit) should be subject to punishment. If you are making money then there is no reason for you to not legitimately purchase software that you use to make a profit.

Piracy also boils down to morals and ethics which is a topic for an entire different essay.

Give people reasons not to pirate and you will reduce piracy but you will never stop it.

# References

[video.google.com/videoplay?docid=-1720068211869162779](http://video.google.com/videoplay?docid=-1720068211869162779) - Lecture by Mark Pesce at the Australian Film Television and Radio School about the future of TV distribution in the age of P2P networks.

<http://cyberinsecure.com/bittorrent-users-are-the-targets-in-new-anti-piracy-scam-emails-spam/> - BitTorrent Users Are The Targets In New Anti-Piracy Scam Emails Spam

[http://www.codefree.com/dvd\\_dvdregionlockingexplained.htm](http://www.codefree.com/dvd_dvdregionlockingexplained.htm) - DVD Regional Locking Explained

<http://www.positech.co.uk/talkingtopirates.html> – Talking to Pirates

3: <http://kottke.org/08/09/why-people-pirate-games> - Why people pirate games

2: <http://consumerist.com/consumer/drm/how-i-became-a-music-pirate-245644.php> - How I Became A Music Pirate

1: <http://forums.sinsofasolarempire.com/341388/get;2078340> – Forum reply to “Want to know why people pirate video games?”

4: <http://www.homemediamagazine.com/web-chatter/piracy-lurks-larger> - “I downloaded and watched True Blood a year before it's been released here in Australia”

5 & 6: [http://en.wikipedia.org/wiki/Digital\\_rights\\_management](http://en.wikipedia.org/wiki/Digital_rights_management) - Digital rights management (DRM) refers to access control technologies used by publishers, copyright holders, and hardware manufacturers to limit usage of digital media or devices.

by preventing access, copying or conversion to other formats by end users.

7: [http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx\\_ag\\_mji\\_0912spore.html](http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html) - Spore's Piracy Problem

8: <http://torrentfreak.com/spore-most-pirated-game-ever-thanks-to-drm-080913/> - Spore: Most Pirated Game Ever Thanks to DRM

9: <http://positech.co.uk/cliffsblog/?p=76> – Replies to a blog post from a game developer “Genuine call for emails from pirates”.

10: [http://en.wikipedia.org/wiki/List\\_of\\_countries'\\_copyright\\_length](http://en.wikipedia.org/wiki/List_of_countries'_copyright_length) - Wikipedia: List of countries' copyright length

11: [http://www.ipi.org/ipi%5CIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/\\$File/CopyrightPiracy.pdf](http://www.ipi.org/ipi%5CIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/$File/CopyrightPiracy.pdf) - Reducing Government Consumption, Increasing Personal Wealth

12: [http://news.cnet.com/8301-13578\\_3-10213367-38.html](http://news.cnet.com/8301-13578_3-10213367-38.html) - Congress looks abroad to curb piracy

13: <http://www.ifpi.org/content/library/DMR2009-key-statistics.pdf> - IFPI digital music report 2009: key statistics

14: <http://www.bsaaustralia.com.au/bsaaweb/cmsimages/Admin/pdf/2007-global-piracy-study-white-paper.pdf> - Fifth annual BSA and IDC Global Software – Software Piracy

15: [http://www.rand.org/pubs/monographs/2009/RAND\\_MG742.pdf](http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf) - Rand Report: Film Piracy, Organized Crime, and Terrorism

16: [http://www.rand.org/pubs/monographs/2009/RAND\\_MG742.pdf](http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf) - Rand Report: Film Piracy, Organized Crime, and Terrorism: pg 47.

17: <http://www.interpol.int/Public/FinancialCrime/IntellectualProperty/Publications/UDF.pdf> – Pages 9 & 10.

- 18: [http://www.rand.org/pubs/monographs/2009/RAND\\_MG742.pdf](http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf) - Rand Report: Film Piracy, Organized Crime, and Terrorism: pg 44.
- 19: [http://www.rand.org/pubs/monographs/2009/RAND\\_MG742.pdf](http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf) - Rand Report: Film Piracy, Organized Crime, and Terrorism.
- 20: [www.ifpi.org/content/library/music-piracy-organised-crime.pdf](http://www.ifpi.org/content/library/music-piracy-organised-crime.pdf) - Music Piracy: Serious, Violent and Organised Crime
- 21: <http://www.itnews.com.au/News/45716,riaa-stung-by-wrongfully-accused-pirate.aspx> - RIAA stung by wrongfully accused 'pirate', By Iain Thomson, 12 February 2007.
- 22: <http://www.wired.com/threatlevel/2008/01/judge-orders-riaa/> - Judge Orders RIAA to Pay Legal Fees to Falsely Accused Lawsuit Target — the Second Such Ruling. By David Kravets, January 17, 2008
- 23: <http://dmca.cs.washington.edu/index.html> - Challenges and Directions for Monitoring P2P File Sharing Networks —or— Why My Printer Received a DMCA Takedown Notice. By Michael Piatek, Tadayoshi Kohno, Arvind Krishnamurthy.
- 24: [http://news.cnet.com/8301-1023\\_3-10256481-93.html](http://news.cnet.com/8301-1023_3-10256481-93.html) - Six months later, no ISPs joining RIAA piracy fight. by Greg Sandoval - June 3, 2009.
- 25: [http://en.wikipedia.org/wiki/List\\_of\\_countries\\_by\\_population](http://en.wikipedia.org/wiki/List_of_countries_by_population) - List of countries by population
- 26: <http://vimeo.com/4739045> - PRA film - The Ghastly Gourmet Cooking Show.
- 27: <http://www.abc.net.au/tv/goodgame/> - Good Game web site.
- 28: <http://www.abc.net.au/iview/> - ABC iView catchup TV service.
- 29: <http://www.uie.com/publications/whitepapers/ImpulseBuying.pdf> - What Causes Customers to Buy on Impulse?
- 30: [http://www.siia.net/index.php?option=com\\_content&view=article&id=171:faq&catid=162:anti-piracy-articles&Itemid=129](http://www.siia.net/index.php?option=com_content&view=article&id=171:faq&catid=162:anti-piracy-articles&Itemid=129) – Anti Piracy FAQ on the SIIA web site.
- 31: <http://www.youtube.com/watch?v=up863eQKGUI> - Don't Copy That Floppy (Official Video - Digitally Remastered)
- 32: <http://www.dontcopythat2.com/> - Don't Copy That Floppy 2, the sequel to Don't Copy that Floppy.
- 33: <http://www.bit-tech.net/news/gaming/2009/09/11/pirated-batman-pc-contains-deliberate-glitch/> – bit-tech.net news article: "Pirated Batman PC contains deliberate glitch" Published: 11th September 2009
- 34: [http://www.abc.net.au/tv/goodgame/video/default.htm?pres=20090720\\_2030&story=1](http://www.abc.net.au/tv/goodgame/video/default.htm?pres=20090720_2030&story=1) – Good Game Web Exclusive Interview - Gabe Newell - Valve Software
- 35: <http://www.techcrunch.com/2008/01/25/global-digital-music-sales-up-40-percent-but-overall-sales-down-10-percent/> - Global Digital Music Sales Up 40 Percent, But Overall Sales Down 10 Percent
- 36, 37, 38: <http://www.theage.com.au/business/digital-music-sales-will-almost-equal-cds-next-year-20090819-epdl.html> - Digital music sales will almost equal CDs next year.
- 39:  
<http://www.dailytech.com/UK+Manager+Says+Major+Labels+Steal+More+Music+Than+Filesharers/article16446.htm> - UK Manager Says Major Labels Steal More Music Than Filesharers
- 40: <http://www.bit-tech.net/news/gaming/2009/10/08/garry-s-mod-sales-performance-revealed/> - Garry's Mod sales performance revealed.
- 41: [http://en.wikipedia.org/wiki/Creative\\_Commons](http://en.wikipedia.org/wiki/Creative_Commons) - Creative Commons Wiki article.
- 42: [http://findarticles.com/p/articles/mi\\_7081/is\\_3\\_26/ai\\_n28457434?tag=content;col1](http://findarticles.com/p/articles/mi_7081/is_3_26/ai_n28457434?tag=content;col1) - Broussard,

Sharee L. (September 2007). "The copyleft movement: creative commons licensing". Communication Research Trends.

43: [http://en.wikipedia.org/wiki/History\\_of\\_hard\\_disk\\_drives](http://en.wikipedia.org/wiki/History_of_hard_disk_drives) - Wikipedia - History of hard disk drives

44: [http://whirlpool.net.au/wiki/?tag=d\\_u\\_m\\_h](http://whirlpool.net.au/wiki/?tag=d_u_m_h) – Whirlpool Wiki - Dialup Modem History

45: [http://en.wikipedia.org/wiki/Bulletin\\_board\\_system](http://en.wikipedia.org/wiki/Bulletin_board_system) – Wikipedia - Bulletin board system

46: <http://www.internetworldstats.com/blog.htm> - Internet World Stats Blog

47: <http://blogs.techrepublic.com.com/tech-news/?p=1651> - Paul Mah, IT News Digest on Tech Republic.com; Majority of Internet bandwidth consumed by P2P services; 28 November 2007.

48: [http://en.wikipedia.org/wiki/Usenet#Usenet\\_traffic\\_today](http://en.wikipedia.org/wiki/Usenet#Usenet_traffic_today) – Wikipedia entry: Usenet

49: <http://en.wikipedia.org/wiki/Sneakernet> – Wikipedia article; Sneakernet

50: <http://creativecommons.org/weblog/entry/24609> - Belgian Band Wins Case Against Theater for Infringing Use of CC-Licensed Song, November 9th, 2010

51: <http://creativecommons.org.au/weblog/entry/269> - Bureau of Meteorology to release water data under CC, November 17, 2009

52: <http://creativecommons.org.au/weblog/entry/254> - DBCDE and Buddie – more open government in Australia, July 20, 2009

53: [http://wiki.creativecommons.org/Case\\_Studies](http://wiki.creativecommons.org/Case_Studies) – CC Case studies

54: [http://news.cnet.com/8301-31001\\_3-20025357-261.html](http://news.cnet.com/8301-31001_3-20025357-261.html) - MPAA, RIAA: Lawsuits won't protect content

55: **Tech News Sites Tout Misleading BitTorrent Piracy Study** - <http://torrentfreak.com/tech-news-sites-tout-misleading-bittorrent-piracy-study-100724/>

56: **Incompetent BitTorrent Researchers Strike Again** - <http://torrentfreak.com/incompetent-bittorrent-researchers-strike-again-101211/>

57: **Economic consequences of movie piracy Australia** - <http://www.afact.org.au/pressreleases/pdf/IPSOS%20Economic%20Consequences%20of%20Movie%20Piracy%20-%20Australia.pdf>

58: **Dead Drops** - <http://datenform.de/blog/dead-drops-preview/>

59: **Amazon S3 storage service** - <http://aws.amazon.com/s3/#importexport>

60: Tanenbaum, Andrew S. (1996). Computer Networks. New Jersey: Prentice-Hall. pp. 83. ISBN 0-13-349945-6.

61: **Comment on “Buzzwords Galore and Bandwidth that May Rival Your Stationwagon”** - <http://dltj.org/article/internet2-hopi-network/#comment-2142>

62: **Pigeon flies past broadband in data speed race - 16 September 2010** - <http://www.bbc.co.uk/news/technology-11325452>

63: **Google helps terabyte data swaps** - <http://news.bbc.co.uk/2/hi/technology/6425975.stm>

64, 65, 66, 67, 68: **IDC WHITE PAPER - The Risks of Obtaining and Using Pirated Software** - <http://download.microsoft.com/download/7/6/9/769E42E0-68C4-4826-838B-0F801DB2EFC2/IDC%20White%20Paper%20on%20Risks%20of%20Pirated%20Software.pdf>

69, 70, : **Study: \$42 billion worth of PSP, DS games pirated** - [http://news.cnet.com/8301-13506\\_3-20006954-17.html](http://news.cnet.com/8301-13506_3-20006954-17.html)

71, 72, 73, 74, 75, 76 77, 78: **Genuine call for emails from pirates** - <http://positech.co.uk/cliffsblog/?p=76>

79: **South Korea government websites targeted in cyber attack** (guardian.co.uk - Friday 4 March 2011)-  
<http://www.guardian.co.uk/world/2011/mar/04/south-korea-websites-cyber-attack>

80: **South Korea hit by cyber attacks** – BBC - 4 March 2011 - <http://www.bbc.co.uk/news/technology-12646052>

81: MPAAs Snags Google Downloading Torrents, Threatens to Disconnect - <http://torrentfreak.com/mpaa-snags-google-downloading-torrents-threatens-to-disconnect-110205/>

82: Makers of 'The Expendables' Sue 6,500 BitTorrent Users - <http://torrentfreak.com/makers-of-the-expendables-sue-6500-bittorrent-users-110208/>

83: US Copyright Group Drops Cases Against Alleged Hurt Locker Pirates - <http://torrentfreak.com/us-copyright-group-drops-cases-against-alleged-hurt-locker-pirates-110118/>

84: Sued BitTorrent Users Score Win In Far Cry Case - <http://torrentfreak.com/sued-bittorrent-users-score-win-in-far-cry-case-101120/>

85: 670 Alleged File-Sharers Off The Hook As BitTorrent Case Dismissed - <http://torrentfreak.com/670-alleged-file-sharers-off-the-hook-as-bittorrent-case-dismissed-110201/>

86: Ubisoft pirates own soundtrack - <http://www.bit-tech.net/news/gaming/2011/03/16/ubisoft-pirates-own-soundtrack/1>

87: Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods - <http://www.gao.gov/new.items/d10423.pdf>

88: Thanks, me hearties - <http://www.economist.com/node/11751035>

89: Look for the silver lining - <http://www.economist.com/node/11750492>

90: <http://torrentfreak.com/5-ways-to-download-torrents-anonymously-100819/> - 5 Ways To Download Torrents Anonymously

91: 'Digital piracy' may benefit companies - [http://www.ox.ac.uk/media/news\\_stories/2008/080317.html](http://www.ox.ac.uk/media/news_stories/2008/080317.html)

92: Tablet maker settles with Microsoft - <http://www.zdnet.com.au/tablet-maker-settles-with-microsoft-339316179.htm>

93: Judge approves settlement in music royalties class action - <http://business.financialpost.com/2011/05/30/judge-approves-settlement-in-music-royalties-class-action/>