

The Shift of Power in the Digital World

Abstract:

Rampant piracy has become an issue in content distribution industries. The cause of financial loss in these industries is blamed on piracy which the consumers appear to be causing. However, a deeper look at this problem reveals a different story. Power has simply shifted from the consumers to the producers. In this shift of power, producers can no longer take advantage of the consumers. The consumers demand to be treated better and piracy is simply a solution to the content distribution industries' inability to understand that they can no longer abuse their power. Those business models which take this shift of power into account, not only gain respect from the consumers, but also reduce piracy by providing better service than the illegal alternatives.

There is a battle stirring in the digital world between the producers and the consumers. The producers, out of touch with the demands of the consumer, are unable to provide services which meet the demands of the consumers. Thus, consumers have turned their backs on the producers' restrictive services and products, and have found other unrestrictive ways to obtain content. Being a producer is tricky in the digital world. Products in the digital world can be reproduced countless times with almost no strain on one's resources. All copy protection schemes to protect digital content have proven to be useless. Thus, the producers have lost the power to enforce restrictions over their content. Looking at how the businesses are coping with this change in the product model, there is a clear distinction between those who have embraced this change and those who are fighting a losing battle. There is a quote which goes something along these lines:

There are two types of engineers. Given an unmaintained path, there are those engineers who will put up a fence and then, there are those who will pave the path.

Many schemes have been implemented by various industries in the digital world which attempt to place a fence around digital products: DRM, copy protection in video games, cd-key verification etc. Very few schemes, if any, have ever succeeded at protecting content from duplication. Often times these restrictions drive consumers away from legitimate vendors and into the hands of piracy. There are even cases of content protection schemes so poorly implemented, that legitimate owners turn to piracy to access content which they should rightfully have access to. The music industry is one of the industries which is having a very hard time coping with this change. It has done so poorly in dealing with this change, that it has created resentment amongst consumers! Digital content cannot be restricted. Those businesses and industries which fail to recognize this and fail to adapt to this change will face extinction. While those who understand this shift in power from the producers to the consumers will learn to satisfy their consumers' demands, and in doing so, create new markets and sources of revenue.

There have been many Digital Rights Management (DRM) schemes implemented in hardware and software. Majority, if not all, have been hacked. One of the early examples of failed DRM is the "Content Scrambling System" (CSS) found on DVDs. Released in 1996, completely hacked by October 1999. This type of DRM was enforced using pure hardware. As with most DRM prevention schemes, a pure software solution was found to get around it. The relative simplicity of the encryption scheme used by CSS helped ensure that it was an easy standard for the manufacturers to follow. Thus, it resulted in players which would have little trouble playing their intended content. But, this simplicity was also the reason why CSS was easily and completely cracked.

Modern DRM however is much more complicated. Blu-ray disks have been promoted as a replacement for DVDs. Blu-ray content has two content protection schemes, AACS and BD+. AACS is a more complex decryption scheme similar to CSS, but with improvements with the lessons learned from the mistakes of CSS. AACS has been cracked, with its encryption keys posted publicly on the Internet. This however, is a temporary attack since old keys can be revoked and new ones issued. Thus, there is a race between the hackers and the content providers in cracking and reissuing keys. The more interesting of the two encryption schemes is the BD+. BD+ allows individual content providers to implement their own decryption schemes which are executed in a virtual machine on players. With this complexity comes flaws in the implementation of the standard. There have been cases where legitimate players were unable to play Blu-ray disks because of poor implementation. As with all schemes, BD+ has also been cracked.

Modern content protection schemes not only enforce DRM on the media but also on the transmission of data. Thus the connection between the players and the displays is also encrypted by a scheme called HDCP. It is designed to prevent a man-in-the-middle attacks. Thus, it is unintuitive to people who are used to analog signals. For analog signals a simple

splitter can allow the signal to be split, while for HDCP encrypted content, a specialized and expensive splitter is needed which itself needs its own power adapter. HDCP is simply an encryption scheme. The type of connection it usually travels on is HDMI or DVI. Many displays were produced with these types of connectors which supported hi-def resolutions before the advent of HDCP. The owners bought these devices with intention to play high-definition content. But with out HDCP decoders, their displays are rendered useless as they can only receive standard definition content. Thus, this created an illegal market for “HDCP strippers.” These devices simply decrypt HDCP content allowing for these legacy displays to work with HDCP. What these “HDCP strippers” have done is simply circumvented HDCP and its “protection”.

This long saga of the battle between video content providers against the duplication of content has been unsuccessful so far. Those who wish to duplicate content are able to do so with little effort, while legitimate users face problems accessing it. The effect of this effort spent in trying to protect content using modern DRM schemes has yet to be fully realized. On one hand this scheme slows down, to some extent, illegal distribution of content. On the other hand, it also pushes away legitimate users from legitimate distribution sources. The reason for the delay in the effect of modern DRM on new content, is that standard unauthorized duplication schemes and resources have not caught up to the demands of HD content in bandwidth and storage. Thus, it is hard to estimate the impact on unauthorized content distribution caused by these modern content protection schemes compared to the lack of resources required to duplicate HD content.

The movie industry has very little respect for legitimate content owners. Enforcing these complicated content protection schemes in which the consumer pays, not only financially, but also emotionally. Often times, legitimately bought media forces the owners to watch FBI warnings and even advertisement prior to experiencing the actual content. One would expect that if they have legitimately purchased content that they not be treated as freeloading pirates. With attitude like this towards their customers, what kind of a result can they expect? Using pirated content allows direct access to it without having to wait for the warning and the advertisements to pass. Even if the cost of pirated content was equal to the legitimate, the consumers would still prefer the pirated and quite possibly prefer it, even if it was more.

The industry goes as far as to pretend that the world is no longer connected. Releasing content in one continent and another continent having to wait months to have it released in there own, only drives people further into the hands of piracy. Simply put, just as the producers took advantage of their power over content distributions, now with the shift of power towards the consumers, the producers should not expect any different from their consumers. Being ethical or not, it is simply natural to optimize one's resources, time and money. The industry needs to respect their consumers and understand their demands. It needs to position itself so it can offer better service then the pirates.

As much as the movie industry complains about loss of revenue through piracy, it is hard to over look the fact that movie theaters are always packed. In a free market, expensive goods indicate great demand. Looking at the cost of popcorn and other condiments, it is clear that the movie theaters are experiencing great demand. In other words, if the service is correctly aimed at the consumer, they are happily willing to pay for it. Loosing business to piracy could be countered not by modifying the product, but by enhancing the service.

The software industry is another industry fighting against unauthorized duplication of content. There battle is quite different then the audio and video industries'. In order to present content, the audio must be heard and the video must be displayed. In doing so, one can simply capture the end product to duplicate content. Software on the other hand, is an experience and cannot simply be captured as such. Thus, in order to duplicate the content, one must copy the original source bit by bit.

Software developers face a completely different challenge in protecting there content. Instead of having control over the hardware, one must design their content for generic hardware. They must completely rely on DRM implemented in software. The software with the most control over the hardware is the operating system. If the operating system is hard to secure, any software written within it cannot be any easier. Microsoft Windows is by far one of the most illegally duplicated operating system. Microsoft, in recent years, has implemented “Windows Genuine Advantage” (WGA) to prevent illegal use of their operating system. WGA works by assigning each user a unique cd-key. Upon installation, that key is associated with the computer's hardware configuration. Every time the computer needs to use Microsoft's online services, such as software updates, this hardware-cd-key pair is validated. WGA is updated every so often and is usually cracked within 24 hours of the release of the update. This crack usually prevents Windows from complaining about the illegal use of their product, but does not allow a user to access Microsoft's services as a normal user would. Often times updates must be hunted down on shady, possibly virus ridden web sites. Legitimate users often run into the same problems as illegitimate users. Due to the hardware-cd-key combination, frequent hardware updates often leads to problems. Users which upgrade there computer hardware often, find themselves being denied full access to a product which they paid for. One must call up Microsoft and explain to them why they need to reset the hardware-cd-key combination. The success or the failure of this approach can only be judged by Microsoft themselves. With the introduction of competitive “free” operating systems, the effects of their restrictions being so visible to legitimate users, have yet to set in. It should be noted that the reason there exists a difference in the usability of Windows between legitimate and illegitimate users, is due to fact that they also provide

online services with their product. Something that cannot be simply cloned.

There are platforms for which software is developed, which are not so common. Majority of these are video games consoles. The Macintosh platform, to some extent, also falls into this category, but with their recent switch to the x86 architecture, are now on a much more common platform. New phones like the iPhone also fall into this category.

Video game consoles' media usually comes on a standardized disks such as a cd-rom, dvd-rom or blu-ray. Some however, use proprietary cartridges and disks. Almost all proprietary platforms, even proprietary format based, have been compromised. All of the proprietary cartridges have either been re-manufactured or have been circumvented by using some other types of media for content distribution. Following the development of some the projects aimed at compromising hardware, it is clear the intention of compromising these system is not to duplicate content, but instead to allow the hardware to perform tasks not intended by its developers. This community is called the "homebrew" community. Upon having the system compromised, then work on content duplication begins. In order to compromise the system, either hardware has to be modified or a software bug has to be found. From the perspective of the user, both of these can end up voiding the product's warranty. Depending on the quality of the product, this is also taken into consideration when deciding whether to compromise the system or not. The Xbox 360 is an example of a product with unusually high failure rate. The user must decide between possibly buying multiple systems or spending money on games.

In majority of these situations, the consumers' motivation to compromising the system clearly seems to be for content duplication. There are also cases where systems are compromised simply to allow it to do what it wasn't designed to do. The reason here is that "I should be able to use what I paid for to the fullest extent." The goal in these situations is to get the system to run an open source operation system such as Linux. The original Microsoft Xbox is a reliable and now, a very cheap system. Thus, Xboxes are widely used as DVR frontends by running programs such as MythTV on them. As elegant as the iPhone is, the developers inexplicably left out a simple and very useful feature on their platform. The ability to copy and paste. By compromising the iPhone, this feature is available through custom add-ons. In other words to use this common feature one has to compromise their iPhone, which not only allows the compromised phone to copy and paste, but also allows the use of unauthorized software.

An interesting note about how Microsoft dealt with compromised Xbox 360's is that, they simply pushed out a software update which detected if a system was compromised or not and then banned them. This ban prevents compromised consoles from playing online. Thus, pirated games can only be played offline. This essentially split their market into two, the offline and the online. The power that they have is due to the online service which they provide. This however, was also circumvented. Hackers have made it so that even the compromised versions look legitimate to the tests done by the updates. Microsoft periodically comes out with updated tests. Thus, once again this has become a cat-and-mouse game.

Not all proprietary systems have been compromised so that illegally duplicated content can be used. The Sony Playstation 3 (PS3) has yet to be added to the list. There are three factors which might be contributing to the lack of motivation to compromise the system. As mentioned earlier the initial push to compromise a system comes from the want to have the system do what it was not intended to do. Almost all projects aim to get Linux to run on the system. The PS3 on the other hand allows one to run a custom operating systems out of the box. Even though this access is restricted as to what hardware one is able to access, which prevents piracy, it is also open enough for the "homebrew" community. If motivation to compromise truly comes from duplicating content, then the format and the size of the content might be playing a role in the lack of motivation to compromise the system. Each game is estimated to be over tens of gigabytes. This might not be a heavy factor with current Internet speeds. The blu-ray format on which the content is stored might be. A blu-ray writer costs about \$200 and a single read-writable disk costs about \$15 at the time of this writing. With time, these costs will only go down. Thus, the heavier factor for the lack of motivation, appears to be that the system conveniently allows one to run "homebrew" software out of the box. Users motivated to play unauthorized content for the purposes of not paying for it, will eventually compromise the system, but they will have little help from the "homebrew" community.

Content protection in the software industry is close to impossible. Whether using standard hardware or customized hardware, if there is a need to remove content protection, there is very little what one can do to prevent it. These fruitless efforts can even end up reducing the quality of the product compared to its pirated counterpart. As an informed consumer, sometimes it can seem foolish to even buy legitimate content over pirated one. Some even pirate content after having paid for it. The business models which are successful in suppressing loss of revenue due to piracy, need to take into account the demands as well as the capabilities of its consumers. Unlike the iPhone which encourages unauthorized use, the PS3 suppresses the need to, by offering an open platform to begin with.

Microsoft dealt with compromised systems by using the power of online services, but it eventually lead to a cat-and-mouse game. This was a poor implementation on Microsoft's part, because there exists an implementation of such services which completely prevents piracy for online applications! This system works by assigning each purchase a unique key. Upon accessing the online service, this key is presented and locked until one disconnects from the service. Once the key is locked, no other user can access the system with the same key. The local software which provides access can be

distributed freely! This solution is as close to the model of physical objects from the perspective of the users as possible. Users can share keys if they wish and makes them feel as if they are not locked down to specific system or location. There are rare problems with this type of configuration. If the user loses the key, or if someone else “steals” it, they have essentially lost the product! Plus, personal computers are very hard to secure these days and if this type of an application is used on a hijacked computer, one can easily have the key stolen. There have been cases of key farming done by botnets, where massive amount of keys are stolen and resold. A simple solution would be to allow a user to reset a key and discard the lost or shared key.

Recently there have been some single player games which have tried the same concept. From the perspective of the users, this is considered “phoning home.” Which could be construed as invasion of privacy. In order to play the single player game, one would need to have an Internet connection. This may seem like something which would not cause any problems since most users today have Internet connections, but for those who don't, it leaves them no option. Even in scenarios like this hackers are able to remove the online validation feature. Thus, this is another case where pirating the product is a better solution than to obtain it from legitimate sources.

The music industry has had great trouble dealing with changes brought in by the digital age. Part of the reason is that music, is an art form. Placing a price on art is almost always impossible. When it comes down to measuring its value with material goods, there is no real metric or scale for conversion. Often times this is seen negatively as normal business models do not work well, but if the right strategy is applied, one can achieve much more.

A band called Radiohead recently did an experiment with the release of their new album, “In Rainbows.” The experiment involved releasing the album online and allowing the users themselves to decide what they wish to pay for the album. With the possibility of downloading it for free. The downloaded music was simply a zip file with mp3s in it. No DRM or any content protection scheme was applied. An article on www.nme.com does a good review of the experiment.

According to reports most fans chose to pay nothing to download the album. However, it still generated more money before it was physically released (on December 31) than the total money generated by sales of the band's previous album, 2003's 'Hail To The Thief'.

...Radiohead's management were monitoring the average price daily, and was prepared to cancel the download facility if the average price became too low.

...The download facility was taken down after three months, and the album went to Number One in the UK and USA after being physically released.

...Warner Chappell concluded that the new release style was a financial success, but did not reveal whether Radiohead plan to release an album in a similar way in the future.

<http://www.nme.com/news/radiohead/40444>

It is interesting to see that even given the offer of free content, due to the respect and admiration of the art, the fans paid their respect by paying for the content. There is very little in service that one can provide in the music industry as an artist, but simply treating their fans with respect was enough.

Majority of the service in the music industry is provided by the content distributors. In recent years, online music distribution has taken off. There are a variety of services which provide content packaged according to their own business model. There are a few factors which a user might consider before joining such a service. Pricing is generally either done per song or album, or unlimited download. Target devices, range from computers to types of mp3 players, car stereos and cell phones. DRM, ranges from some who have DRM on all sold media to some that offer mixed and to others who offer content without DRM.

iTunes is a widely used music distribution application created by Apple. It supports the Windows and the Mac operating systems. Some of the music purchased from iTunes uses the FairPlay DRM scheme. While the rest can be downloaded in the open AAC file format. The FairPlay DRM is only available in the iPod and a few cell phones. Some of the restrictions imposed by the DRM as quoted from wikipedia:

Users can make a maximum of seven CD copies of any particular playlist containing songs purchased from the iTunes Store.

Users can access their purchased songs on a maximum of five computers.

Songs can only be played on a computer with iTunes or an iPod; other MP3 devices do not support FairPlay

encoded tracks.

There are no restrictions on number of iPods to which a purchased song can be transferred nor the number of times any individual song can be burned to CD.

http://en.wikipedia.org/wiki/iTunes_Store#Pricing_model

Like all DRM, this has also been cracked. There are programs which simply strip out the DRM allowing arbitrary players and users to play the content. It is interesting that they placed no restrictions on the ability to create audio cds for music encrypted by FairPlay. This implies that, one can simply create an audio cd, and then reconvert the audio tracks into any file format. A simple way to remove the content protection scheme.

It is very interesting how the DRM scheme implemented by iTunes satisfies the needs of the users as well as the needs of the producers. From the perspective of the users, they are able to do almost everything with the DRM music as they would do with unrestricted music. They were even able to convert it to unrestricted music without the need for special software to strip the DRM. Being able to access the music from up to 5 computers and the lack of restriction on number of iPods the music is transferred to, leaves the user with little else to desire. With the explosion in the adaption of iPod, the restriction that very few handheld devices can use the FairPlay DRM, to most users, has become a moot point. Producers on the other hand, see the size of the iTunes market and are willing to lower the restrictions on their content. The restrictions exist because it gives them a sense of security. It should be noted that the pricing model is also very competitive.

Apple's image is based around customer satisfaction. This image clearly shows in the application of DRM in their iTunes store. In addition to the relatively forgiving DRM, Apple has come on the news several times, claiming that it is in talks with producers to try to lower the DRM restrictions and to lower the price of the music. Thus, consumers see Apple as a company dedicated to customer satisfaction. Apple understands the shift in power in the digital world from the producers to the consumers. In adapting to this change and convincing part of the music industry to follow, Apple has created a very successful business model.

As much as there is the success of iTunes, there are many failures as well. Yahoo and Walmart had to shutdown their online music stores due to lack of interest from customers. Their DRM servers were taken offline as well. This meant that all DRM music purchased from the stores would no longer work! Their "work around" was to copy the music to audio disks. Something that is generally done by pirates to "steal" music and is a great inconvenience if one's library was large. This resulted in customers who could no longer trust content protected media. These failures continually force the users to turn to piracy and away from legitimate sources. From the success of iTunes it is clear that there is demand for online music distribution, but with mismanaged business practices, the industry will face hard times.

In recent years, there have been a number of Internet startups which aim solely to satisfy the customer. YouTube was a startup which allows users to post small video clips online. The video clips are then viewable to everyone. They even have a feature which allows clips hosted on YouTube, to be played on any website. As of now the clips viewed from other sites, have very little advertising if any. This type of an open and free business practice caused a boom in the use of the service. From this great success, YouTube was bought off by Google.

In some cases clips were posted on YouTube which were from tv shows and other copyrighted content. The entertainment industry was not going to allow such freedom of their content. A company called Viacom which owns several movie studios and cable channels, decided to sue YouTube. YouTube's policy on copyright infringement is that, if one's content is found to be copyrighted, one can contact Google and inform them of it. Google will take down the content. This case is discussed in detail by cnet news.

Although legitimate copyright concerns come into play, Viacom's action is "probably about a large company that would prefer the old status quo, where they had most of the control (over their content distribution), and they didn't cede it to companies like YouTube and Google," said Jeffrey Lindgren, an intellectual-property lawyer at Morgan Miller Blair in San Francisco.

Nonetheless, Viacom says in its complaint that YouTube failed to prevent its users from posting pirated material to the site. San Bruno, Calif.-based YouTube will remove clips that feature unauthorized material only after it receives a takedown notice from the copyright holder, Viacom said.

This, many entertainment executives say, is unfair. YouTube's policy, which the company says complies with copyright law, forces many of the biggest studios to devote time and money toward policing someone else's site. Often, no sooner than a company asks YouTube to take down a clip, users post a new version of the same clip.

Google lawyers said they are relying on a 1998 law called the Digital Millennium Copyright Act (DMCA) to shield them from liability. One provision of that statute generally says companies are off the hook if they remove copyrighted content promptly when it is brought to their attention.

YouTube was also expected late last year to release a technology that would automatically weed out copyright content from the site. NBC's Zucker and others in Hollywood have accused the company of dragging its feet. Viacom said that only when an agreement is reached will YouTube begin safeguarding an entertainment company's copyright property.

http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html

Viacom has all rights to protect its content. The system implemented by YouTube, as advised by the "Digital Millennium Copyright Act," is clearly a nuisance to agencies whose content is being illegally distributed by the YouTube service. Users can simply repost removed content. Thus, catching these users and their content has become a cat-and-mouse game. YouTube is planning on releasing an automatic filter to counter such users.

As pointed out by Jeffrey Lindgren, corporations like Viacom are simply scared to loose control over the distribution of their content. Viacom appears to have acknowledged the idea that there is a shift in power from the producers to the consumers. After having YouTube remove their copyrighted content, they started their own online content distribution services. It is obvious that preventing the content from being distributed on the Internet is close to impossible. Thus, producing a competitive service, compared to services which could be provided by illegal distributors, is clearly a step in the right direction. Many of the services created by Viacom share the same features as YouTube. Such as being able to comment on video clips, to being able to display the video clips on other websites. The distribution services created by Viacom, do however sometimes force users to watch advertisements. Websites like hulu.com and comedycentral.com were created to regain some control over the online distribution of content. From the perspective of the user, these services are almost exactly what one would expect from a service that distributed video clips online. Thus, illegal distribution of these clips is slowing down.

These services however are not without mistakes. Some of these sites only offer services to specific users based on their geographical location. Thus, popular shows have become big targets for illegal distribution. Once again, to rectify this situation, all that is needed to be done is to recognize that the world has become smaller with the advent of the Internet. The differences of living in one geographical location verses another, from the digital content distribution's perspective, are very small. Thus, failure to meet the demands of the users, leads to the loss of control over the distribution of one's content.

Digital content is something which cannot be controlled. From the various schemes applied by video distributors, to the schemes applied by software distributors, all have failed to protect the content from being duplicated. Instead of punishing illegal distributors and consumers, these schemes instead end up punishing those who obtain content legitimately. Illegal distributors should be treated as competition. If they are capable of supplying content with better service then the legitimate distributors, then there is clearly something wrong the distribution model. Legitimate distributors' services have not caught up to the level of service provided by illegal distributors. Even if consumers paid for the illegally obtained content, they would still prefer it over legitimate content. With the ease of use provided by pirated content, there is no economical reason to use legitimate content. In order to counter piracy, one not only needs to provide high quality content, but also high quality service. Both of which can be achieved if one begins to understand the shift of power from the producers to the consumers and reacts appropriately to meet the needs of the changing market.

Pollock, Rufus *P2P, Online File-Sharing, and the Music Industry*. 31 Mar. 2006
<http://www.rufuspollock.org/economics/p2p_summary.html>

LaGesse, David *Wal-Mart Shuts Down Online Music Store, Stranding Customers*. 30 Sept. 2008
<<http://www.usnews.com/blogs/daves-download/2008/9/30/wal-mart-shuts-down-online-music-store-stranding-customers.html>>

Yahoo: Burn your DRMed tracks to CD now. 28 Jul. 2008
<http://www.tamilstar.info/news/publish/article_10265.shtml>

Broache, Anne and Sandoval, Greg *Viacom sues Google over YouTube clips*. 13 Mar. 2007
<http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html>

Axon, Samuel *PlayStation Home hacked, the search for backup exploits begins*. 23 Oct. 2008
<<http://www.engadget.com/2008/10/23/playstation-home-hacked-the-search-for-backup-exploits-begins/>>

Delahunty, James "Dela" *Microsoft says Xbox Live will counter hacking efforts*. 9 Aug. 2006
<<http://www.afterdawn.com/news/archive/7816.cfm>>

Microsoft's anti-piracy push gets personal. 23 Oct. 2008
<<http://www.news.com.au/technology/story/0,25642,24539702-5014239,00.html>>

Wikipedia: Content Scramble System.
<http://en.wikipedia.org/wiki/Content_Scramble_System>

Wikipedia: Advanced Access Content System.
<http://en.wikipedia.org/wiki/Advanced_Access_Content_System>

Wikipedia: BD+.
<<http://en.wikipedia.org/wiki/BD%2B>>

Wikipedia: iTunes Store.
<http://en.wikipedia.org/wiki/iTunes_Store>

Wikipedia: FairPlay.
<<http://en.wikipedia.org/wiki/FairPlay>>

Wikipedia: Xbox Modding.
<http://en.wikipedia.org/wiki/Xbox#Xbox_modding>