

Digital Rights Management: Flawed at Best

Just prior to the turn of the century, as the internet became more reliable, storage became cheaper, and compression technology advanced, online file sharing developed as an attractive way to distribute files between peers.¹ By 1999, early peer-to-peer (P2P) file sharing services such as the original Napster had made their presence known to the United States entertainment industry,² who alleged that this drastic increase in the sharing of digital media endangered their profit streams, and thus their ability to produce quality content.³ Since the Napster trial, file sharing has grown to incredible proportions. The MPAA estimates that in 2005, movie piracy cost the industry as a whole \$18.2 billion,⁴ and is now an epidemic that has struck the western world. One proposed answer to the problem of piracy is the Digital Rights Management (DRM) system, a wrapper for digital media files that attempts to prevent sharing and use of digital media by unauthorized persons.⁵

In his book 'Beyond Fear,' security and cryptography expert Bruce Schneier defines a security system as a "set of things put in place, or done, to prevent adverse consequences... [arising] from the intentional and unwarranted actions of others."⁶ The author goes on to outline a five step plan that allows the value of any potential security measure to be thoroughly analyzed. At their core,

DRM schemes are no more than software security, built to protect digital media files from unauthorized distribution and use.⁷ Throughout the remainder of this paper, Schneier's plan will be utilized to analyze their effectiveness as piracy preventatives.

Step 1: What assets are you trying to protect and how?

The basic DRM system consists of a client, a license, and some encrypted content, usually a digital media file. When a client obtains protected content, he also obtains a license that specifies what can and cannot be done with that content. Upon attempting to utilize the protected media, the content player analyzes the content and license, ensuring that the intended actions of the client are allowed by the license.⁸ If this is the case, the player uses an encryption key contained in the license to unlock and play the content. If the client is not authorized, the content player will often direct the user to a license server where he can obtain a valid license.⁹ Licenses and players are generally authenticated to only one computer via some unique identifier, and are not transferrable between machines.¹⁰

An alternative to encrypted DRM packages has been proposed in the form of digital watermarking schemes. These embed a unique identifying mark in a digital file at the time of creation that can be read by players at a later date. If a watermark is found, the player can then restrict user action or demand a valid license before cooperating.¹¹ These systems are usually less effective than their

encryption-based brethren, as they generally preserve the structure of media files and can be simply ignored by third party players that do not support the standard. Additionally, recompressing or transcoding the file to a different format is often enough to destroy the fragile watermark, making it unreadable.¹²

In October of 1998, the United States passed the Digital Millennium Copyright Act (DMCA), which includes an anti-circumvention clause that makes breaking DRM systems illegal.¹³ Likewise, development, description, and distribution of tools designed to defeat DRM are also defined as criminal acts.¹⁴ Repeat offenders under the act, or those who break the act in seek of financial gain can be subject to up to ten years of imprisonment, and a fine of up to one million dollars, as well as restitution of lost profits to the copyright holder.¹⁵ Opponents of the law imply that it is the direct result of entertainment industry lobbying, and a disaster for innovation, free speech, competition, and fair use.¹⁶

The defenses provided by the DMCA have spawned a slew of protected content in the marketplace, including digital video and audio files, eBooks, and recently, some television content.¹⁷ Vendors of DRM systems tout the benefits of their products with adjectives like flexible, secure, transparent, and open,¹⁸ while consumer rights advocates like the Electronic Frontier Foundation claim that even when a protected product has been legitimately purchased, it is still owned by the distributor, who retains the right to modify the DRM scheme at any time. As such, these opponents of the practice argue that DRM violates the fair use

and first sale rights of consumers as outlined in traditional copyright law,¹⁹ while doing nothing to prevent piracy.²⁰

Until recently, the vast majority of legally available digital content, especially that which was distributed online, has been protected by some form of DRM system. Examples include the now defunct Microsoft Plays for Sure program, the Napster 2.0 subscription and download service, the Real Music online store, and most notably, the Apple iTunes Store.²¹ CEO Steve Jobs maintains that DRM protection for purchased content is mandated by record companies in their licensing agreements with Apple, but that he and his company would readily embrace the abolishment of DRM on their wares.²² Within the last year, the music industry has broken its previous stance by allowing the Amazon.com online music store to sell unprotected Mp3 files. Industry analyst Phil Leigh claims that "The labels think Apple has too much influence," pointing to the latter's near 80% market share as evidence of his claim. Many postulate that the move was not recognition of the failures of DRM, but rather, a strategic business decision meant to remove some of the stranglehold that iTunes has on the legal music download market.²³

Meanwhile, the adult video industry has recently proposed a more liberal system of DRM for their content that seeks only to encourage a user to purchase content once, but not to protect it thereafter. The program allows users to purchase and download video content directly from an online store, at which

point the user can do nothing with the file but burn it to a DVD, and then only once. The hope is that this system will encourage users to legitimately purchase films instead of illegally downloading them, as it combines the convenience of downloads with the freedom of owning a physical copy of the film whose protection is non-intrusive.²⁴

Step 2: What are the risks to these assets?

People have always shared physical objects of value. However, recent advances in computer and compression technologies have transferred the perceived value of an object from the physical format to its digital representation.²⁵ Prior to the mid-1990's, file sharing took place via the so-called "Sneaker-net" distribution model, wherein audio cassette tapes and floppy diskettes were shared almost exclusively in physical format between friends. In technical terms, the threat of this network was minimized by its high latency (peers had to either meet or send content by mail or courier), lack of a central search engine, and the fact that cassette tapes lost fidelity when copied. For these three reasons, the Sneaker-net was never widely investigated or prosecuted,²⁶ but was considered in need of improvement by its users.

Enter the Darknet: "A collection of networks and technologies used to share digital content,"²⁷ wherein the propagation of powerful compression algorithms and high speed networks has permanently shifted industry perception of file sharing from casual and non-threatening to dangerous and highly illegal.

This new form of distribution is faster, searchable, and wide spread, enabling people who had never met to exchange files, including copyrighted works. The first content shared on the internet was primarily hosted on central servers unknowingly maintained by large institutions, such as universities and corporations. These all but disappeared when it was realized that they made easy targets for entertainment industry copyright lawyers.²⁸

In 1999, a free peer-to-peer (P2P) service called Napster simultaneously improved upon the central server model and brought file sharing into the mainstream, much to the torment of the entertainment industry.²⁹ The application revolutionized file sharing by distributing bandwidth use and making all available content searchable, but still maintained a central database of all available files that led to its eventual prosecution and shutdown.³⁰ However, by the time Napster was taken offline, file sharing had become a popular activity among college students and young people, and many other applications rose to fill the void it left behind.

One such service called Gnutella fixed the vulnerability of maintaining a centralized database system by fully distributing its object and peer index across multiple user-run network nodes.³¹ Joining the network and searching for a file was accomplished via a recursive process called query flooding; a design choice that once more reduced the bandwidth requirements of users, as well as the latency of the network as a whole.³² Many applications such as Limewire and Kazaa soon implemented the Gnutella protocol and were the cause of much attention, as without a central server, they were hard to shut down, but still

enabled illegal piracy. Furthermore, unlike Napster, these services positioned themselves as enabling distribution of legal content, challenging the view that P2P applications were only useful for breaking the law.³³

The file sharing story continues with the release of the BitTorrent protocol, by far the most popular P2P protocol in use today.³⁴ By some conservative accounts, up to 30% of all internet backbone traffic is a result of the service,³⁵ which has been implemented in numerous applications and is cause of great concern for the entertainment industry.³⁶ BitTorrent further improves upon the P2P distribution model by entirely removing the need to maintain a central server or network structure. Each file being downloaded has its own constantly changing network, called a Swarm, and one must only locate a tracker (a server that maintains a list of peers in the Swarm) in order to join.³⁷ The constantly changing network structure and the fact that any person can set up a tracker makes BitTorrent hard to police, although some Canadian ISP's have recently begun to severely throttle BitTorrent traffic, to much outcry from customers.³⁸

The Recording Industry Association of America (RIAA) decries digital music piracy as “too benign term that doesn’t even begin to adequately describe the toll that music theft takes on the many artists, songwriters, musicians, record label employees and others whose hard work and great talent make music possible.” The group attributes an annual \$12.5 billion in global economic loss, along with over 72,000 worker layoffs to piracy.³⁹

Step 3: How well does the security solution mitigate those risks?

When researching the Darknet phenomenon of widespread file sharing, one truism established by the Microsoft Research group was that any interesting or popular content that was produced would be leaked onto file sharing networks. This, they proposed, would be due to users who either possess enough ability to break any protection placed on the object, or those who have access to the objects before protection is applied.⁴⁰ Contrary to this observation, DRM vendors consistently claim that their products are aimed at the average user and not determined pirate groups. Meanwhile, any user who can perform a web search or figure out how to use a P2P application can get unfettered access to all of the material that other, more determined people have helpfully unlocked.⁴¹

In the continental United States, entertainment industry lobbyists and litigators seek to combat this effect by bringing lawsuits against those who violate the anti-circumvention clause of the DMCA. One of the first arrests under the DMCA was that of Russian programmer Dmitry Sklyarov, who was charged in 2001 with ‘trafficking in, and offering to the public, a software program that could circumvent technological protections on copyrighted material.’ While working at Russian software development company ElcomSoft, Sklyarov had co-written an application called The Advanced eBook Processor that was capable of breaking the DRM on Adobe Systems’ popular Portable Document Format (PDF). The charges against Sklyarov and ElcomSoft were later dropped when it was decided that the DMCA did not apply in Russia.⁴²

Shortly thereafter, Norwegian programmer John “DVD John” Lech Johansen wrote a Linux-based utility called DeCSS that stripped the Content Scrambling System (CSS) DRM from DVD movies.⁴³ At the time, the body that regulated DVD licensing and the CSS system had not arranged for a license for the Linux operating system, so Johansen and a group of friends took it upon themselves to write a utility that would allow them to watch DVDs on their computers.⁴⁴ He too was arrested under the DMCA but later released, on the grounds that under Norwegian law, DeCSS complied with the fair use allowances of copyright law.⁴⁵

All DRM systems as we know them are inherently flawed. In cryptographic terms, they put the ciphertext, algorithm, and key in the hands of the attacker, and expect to stay unbroken.⁴⁶ In the words of EFF speaker Cory Doctorow, “hilarity ensues.” Add the anti-circumvention clause of the DMCA to the mix, and even if an algorithm is found to have a weakness, it cannot be explored or published under threat of law, leading to an un-improving sequence of poor, easily broken systems.⁴⁷ In his many speeches to audiences around the world, Bill Gates has told audiences that current DRM schemes have “huge problems” and that fans “should just buy a CD and rip it” to ensure that they can use their media however they like without challenging the law.⁴⁸

Additionally, most software DRM systems are not break once break everywhere (BOBE) resilient. This means that the knowledge gained in breaking

one instance of the system can be easily applied to breaking all other instances, leading to widespread class breaks.⁴⁹ Security consultant Bruce Schneier refers to these types of security systems as being brittle, noting that they often fail poorly, and are not dynamic enough to adjust to new situations.⁵⁰ Jim Griffin, a music industry consultant and former Geffen Records employee, has been quoted as saying that “every time a 42-year-old figures out how to lock something up, a 14-year-old is going to figure out a new program [to unlock it].”⁵¹ Since the vast majority of commercial DRM systems fall into this category,⁵² almost all have been broken, often within weeks of their release.⁵³ An ongoing field of research is renewable DRM systems that can be updated in the field in the case of a cryptographic breach.⁵⁴

Even if a DRM system is successful in standing up to determined crackers, the media that it protects is often available in other, poorly protected formats, meaning that unless strong DRM systems are government mandated world round, content will continue to find its way onto the internet.⁵⁵ As an example, conditional access content delivery systems like cable, satellite television, and satellite radio provide very little protection to media when used by a legitimate, paying user. Any post-unlock protections such as Macrovision are trivial to defeat, allowing the user to do most anything with the content.⁵⁶ Traditionally, physical media formats like compact discs, cassette tapes, vinyl records, and books are also unprotected by DRM, making the process of sharing them with others trivial in nature.⁵⁷

Experts in the field agree that the file sharing networks are here to stay, and will continue to thrive and improve in correlation with increased broadband internet adoption.⁵⁸ As networks improve, they become more attractive to users, who see an increased amount of available content in return for the small, relatively static cost of an internet connection.⁵⁹ As such, DRM systems, specifically strong ones, present a disincentive to those who are already involved in file sharing – They introduce both a monetary and freedom cost to something that initially had neither.⁶⁰ If competing with the P2P file sharing phenomenon, it is thought in some circles that more money could be made by selling unprotected files, and competing on the terms of the networks themselves.⁶¹

Steps 4 and 5: What other risks, costs, and trade-offs does the security solution create?

Digital rights management systems are bad for customers. They force otherwise honest, legitimate customers to choose from an ever increasing multitude of formats⁶² that are all limiting in nature,⁶³ and drive frustrated customers toward file sharing as a way to get media whose use is not limited.⁶⁴ Although the DMCA explicitly states that “nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use,”⁶⁵ it has had many unintended consequences that directly impact fair use, free speech, competition, and innovation. Were this law to be strengthened by legislation mandating support for DRM in all media playback devices, the

entertainment industry would be given unlimited veto power over what new technology is brought to market.⁶⁶

DRM backed by licensing agreements and enforced by the DMCA prevents reverse engineering of devices, and promotes vendor lock in, potentially leading to market stagnation.⁶⁷ Sir Timothy Berners-Lee, inventor of the internet, has been quoted as calling the DMCA anti-competitive, saying that “it gives copyright holders... the legal power to create closed technology platforms and exclude competitors from interoperating with them.”⁶⁸ In 2004, RealNetworks released its Harmony technology, a DRM system that allowed songs purchased at its online Real Music Store to be played by many of the portable devices available at the time, including the Apple iPod.⁶⁹ This interoperability had not been possible before, and Apple lashed out at RealNetworks, accusing them of adopting “the tactics and ethics of a hacker” to reverse engineer their FairPlay DRM system,⁷⁰ recognizing that the move broadened and diversified the choices available to iPod owners.

Device lock-in can also harm companies’ market share and reputation with their customers. Before the release and subsequent wide adoption of the Mp3 format, the Sony Corporation was the unquestionable leader in portable music players, due to their incredibly successful line of Walkman devices. However, while other companies released portable players that utilized the widely adopted Mp3 format, Sony refused,⁷¹ preferring instead to offer support only for their

proprietary ATRAC format. While technologically superior to Mp3,⁷² ATRAC was wrapped in OpenMG DRM, forcing users to support inferior Sony products and software in order to enjoy their music collections on the go.⁷³ Market performance of the players was dismal, paving the way for the Apple iPod to take and hold market lead.⁷⁴

Most DRM systems also include hidden fees in their pricing structures and cause legally purchased media to 'expire' after a certain number of operations. For example, both Apples' iTunes Store and Napster 2.0 impose a hard limitation on the number of 'unique' devices that a file can be copied to.⁷⁵ If a user is a good customer and purchases the newest computer available every few years, she can quickly run into this limitation. On the other hand, if the customer is hapless and unlucky, he may need to reformat his machine once a year and can also easily run out of copy operations.

One traditionally preserved right under copyright law is that of first sale, now all but removed by licensing agreements. Because digital content is generally licensed to a particular user rather than sold, there is no avenue by which it can be resold, shared, or simply given away without violating the terms of the licensing agreement.⁷⁶ Along with first sale, traditional copyright law also guarantees the user the right of fair use. This allows media to be backed up for personal use, parodied, criticized, commented and reported upon. However, if

the media in question is protected with DRM, the scheme must be broken to exercise the right of fair use, thus violating the DMCA.⁷⁷

This pairing of technology and law has also had a general scare effect on the academic community, including researchers, journalists, scientists, software engineers, and librarians. It has been misused to prosecute creators of third-party software, as well as to silence researchers pointing out flaws in systems, and journalists publishing protected code.⁷⁸ Even though the law includes exemptions for certain works that are revisited and updated every three years, many consider them to be too narrow, potentially targeting the work of academics and scholars.⁷⁹ Recall the previously mentioned case against Dmitry Sklyarov, who was arrested under the DMCA while lecturing at a Las Vegas seminar.⁸⁰ After his arrest, the Russian government issued a blanket warning to its researchers, telling them to stay away from American conferences, as they were apparently now a place where certain equations were considered illegal.⁸¹

Conclusion:

Over the course of this discussion, we have seen the conditions that created the file sharing craze, been introduced to the potential solution of DRM, and walked through some of the reasons as to why it is not an optimal one. While the published statistics regarding the damages incurred from file sharing are no doubt based in truth, we have seen that the limited security provided by DRM systems do not justify the obligatory trade offs incurred in their use.

Digital Rights Management schemes supported by the DMCA allow distributors of content to write their own copyright laws that prop up their business plans, flawed though they may be in the digital age. The history of copyright law and technology clashes has shown that regardless of the obvious benefits of new technologies, the media industry and their representatives have always claimed that emerging technologies not supported by their existing profit models will put them out of business.⁸² However, in every case on record, these altercations have led to a revision of copyright law, not a ban on technology.^{83 84} Contemporary copyright law is thought to be supported by the inefficient production and distribution methods of the pre-internet era. In an age when an unlimited number of perfect copies of an object can be created and distributed for nothing beyond the initial cost of production, previous laws need to be reconsidered if they are to still apply.⁸⁵

The basic flaws inherent in every DRM system, the rampant destruction of customers right to first sale and fair use, and the fear of device lock-in and market stagnation lead this author to believe that a better solution need be proposed to protect the intellectual properties of media producers. In his open letter to music fans and the industry at large, Apple CEO Steve Jobs sums up the argument against DRM nicely, pointing out that in 2006, less than two billion DRM-protected songs were sold by online music stores, while in that same period of time, more than 20 billion DRM free songs were sold in the compact disc format. With over 90% of record company revenues resulting from the sale of unprotected CDs, what benefit does DRM have on the remaining 10% of

sales?⁸⁶ In the words Sir Timothy Berners-Lee, “DRM technologies are clumsy and ineffective; they inconvenience legitimate users but do little to stop pirates.”⁸⁷

¹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Pages 4-5.

² Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 5.

³ “Benefits of Windows Media DRM,” *Microsoft Corporation*, <http://www.microsoft.com/windows/windowsmedia/forpros/drm/benefits.aspx>

⁴ “Who Piracy Hurts,” *MPAA.org*, http://www.mpa.org/piracy_WhoPiracyHurts.asp

⁵ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 2.

⁶ Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer Science+Business Media, 2006), Pages 11-12.

⁷ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 12.

⁸ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 11.

⁹ “Benefits of Windows Media DRM,” *Microsoft Corporation*, <http://www.microsoft.com/windows/windowsmedia/forpros/drm/benefits.aspx>

¹⁰ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 12.

¹¹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, “The Darknet and the Future of Content Distribution” (Microsoft Research Group), Page 13.

¹² “The Digital Millenium Copyright Act (DMCA),” *UCLA Online Institute for Cyberspace Law and Policy*, <http://www.gseis.ucla.edu/iclp/dmca1.htm>

¹³ Samuelson Law, “Frequently Asked Questions (and Answers) about Anticircumvention (DMCA),” *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>

¹⁴ Regina Lynn, “A Burning Need for More Porn,” *Wired News*, <http://www.wired.com/culture/lifestyle/commentary/sexdrive/2006/03/70547>

-
- ¹⁵ Samuelson Law, "Frequently Asked Questions (and Answers) about Anticircumvention (DMCA)," *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>
- ¹⁶ "Digital Rights Management and Copy Protection Schemes," *Electronic Frontier Foundation*, <http://www.eff.org/issues/drm>
- ¹⁷ "Benefits of Windows Media DRM," *Microsoft Corporation*, <http://www.microsoft.com/windows/windowsmedia/forpros/drm/benefits.aspx>
- ¹⁸ "Windows Media DRM FAQ," *Microsoft Corporation*, <http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx>
- ¹⁹ "The Customer is Always Wrong: A User's Guide to DRM in Online Music," *Electronic Frontier Foundation*, <http://w2.eff.org/IP/DRM/guide/>
- ²⁰ "Digital Rights Management and Copy Protection Schemes," *Electronic Frontier Foundation*, <http://www.eff.org/issues/drm>
- ²¹ "The Customer is Always Wrong: A User's Guide to DRM in Online Music," *Electronic Frontier Foundation*, <http://w2.eff.org/IP/DRM/guide/>
- ²² Steve Jobs, "Thoughts on Music," *Apple.com*, <http://www.apple.com/hotnews/thoughtsonmusic/>
- ²³ Jefferson Graham, "Amazon takes on Apple with copy-protection-free music," *USA Today*, http://www.usatoday.com/money/media/2008-03-25-sony-music-service_N.htm
- ²⁴ "What is DRM?" *WiseGeek.com*, <http://www.wisegeek.com/what-is-drm.htm>
- ²⁵ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 1.
- ²⁶ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 3.
- ²⁷ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 1.
- ²⁸ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 5.
- ²⁹ James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, (Boston: Pearson Education, 2008), page 153
- ³⁰ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 5.

-
- ³¹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 6.
- ³² James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, (Boston: Pearson Education, 2008), page 154
- ³³ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 6.
- ³⁴ James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, (Boston: Pearson Education, 2008), page 145
- ³⁵ Matt Hartley, "Bell irks ISPs with New Throttling Policy," *The Globe and Mail*, <http://www.theglobeandmail.com/servlet/story/RTGAM.20080325.wqtinternet26/BNStory/Technology/?page=rss&id=RTGAM.20080325.wqtinternet26>
- ³⁶ James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, (Boston: Pearson Education, 2008), page 153
- ³⁷ James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach, 4th Edition*, (Boston: Pearson Education, 2008), pages 149-151
- ³⁸ Matt Hartley, "Bell Irks ISPs with New Throttling Policy", *Globe and Mail*, <http://www.theglobeandmail.com/servlet/story/RTGAM.20080325.wqtinternet26/BNStory/Technology/?page=rss&id=RTGAM.20080325.wqtinternet26>
- ³⁹ "Piracy: Online and On the Street," *RIAA.com*, <http://www.riaa.com/physicalpiracy.php>
- ⁴⁰ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 2.
- ⁴¹ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/anil/stuff/doctorow-drm-ms.html>
- ⁴² "Frequently Asked Questions (and Answers) About the Dmitry Sklyarov & ElcomSoft Prosecution," *Electronic Frontier Foundation*, http://w2.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html
- ⁴³ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 12.
- ⁴⁴ Siva Vaidhyanathan, *Copyright and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity* (New York: New York University Press, 2001), Page 176
- ⁴⁵ "Jon Lech Johansen," *Wikipedia*, http://en.wikipedia.org/wiki/Jon_Lech_Johansen

⁴⁶ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁴⁷ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁴⁸ Cyrus Farivar, "CE-Oh No He Didn't! Part XXI : Gates Tells Consumers to Ditch DRMed Tunes, Buy CDs," *Engadget.com*, <http://www.engadget.com/2006/12/14/ce-oh-no-he-didnt-part-xxi-gates-tells-consumers-to-ditch-dr/>

⁴⁹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 12.

⁵⁰ Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer Science+Business Media, 2006), Page 119.

⁵¹ Jim Griffin, quoted in Sara Baase, *A Gift of Fire, 2nd Edition* (London: Pearson Education, 2003), Page 260

⁵² Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 12.

⁵³ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁵⁴ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 12.

⁵⁵ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 12.

⁵⁶ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 11.

⁵⁷ "The Customer is Always Wrong: A User's Guide to DRM in Online Music," *Electronic Frontier Foundation*, <http://w2.eff.org/IP/DRM/guide/>

⁵⁸ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 2.

⁵⁹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 15.

⁶⁰ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 13.

⁶¹ Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" (Microsoft Research Group), Page 15.

-
- ⁶² "The Customer is Always Wrong: A User's Guide to DRM in Online Music," *Electronic Frontier Foundation*, <http://w2.eff.org/IP/DRM/guide/>
- ⁶³ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>
- ⁶⁴ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>
- ⁶⁵ "The Digital Millenium Copyright Act (DMCA)," *UCLA Online Institute for Cyberspace Law and Policy*, <http://www.gseis.ucla.edu/iclp/dmca1.htm>
- ⁶⁶ "Digital Rights Management and Copy Protection Schemes," *Electronic Frontier Foundation*, <http://www.eff.org/issues/drm>
- ⁶⁷ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>
- ⁶⁸ Sir Timothy Berners-Lee, "Circumventing Competition: The Perverse Consequences of the Digital Millenium Copyright Act," *Cato Institute*, http://www.cato.org/pub_display.php?pub_id=6025
- ⁶⁹ "RealNetworks Introduces Harmony, Enabling Consumers to Buy Digital Music that Plays on all Popular Devices," *RealNetworks.com*, <http://www.realnetworks.com/company/press/releases/2004/harmony.html>
- ⁷⁰ Matt Hines, "Apple Accuses Real over iTunes 'Hacking'," *Silicon.com Security Strategy*, <http://software.silicon.com/security/0,39024655,39122751,00.htm>
- ⁷¹ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>
- ⁷² "ZDNet Definition for: ATRAC3," *ZDNet.com*, <http://dictionary.zdnet.com/definition/ATRAC3.html>
- ⁷³ "ZDNet Definition for: OpenMG," *ZDNet.com*, <http://dictionary.zdnet.com/definition/OpenMG.html>
- ⁷⁴ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation, Hosted by Dashes.com*, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>
- ⁷⁵ "The Customer is Always Wrong: A User's Guide to DRM in Online Music," *Electronic Frontier Foundation*, <http://w2.eff.org/IP/DRM/guide/>
- ⁷⁶ Samuelson Law, "Frequently Asked Questions (and Answers) about Anticircumvention (DMCA)," *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>

⁷⁷ Samuelson Law, "Frequently Asked Questions (and Answers) about Anticircumvention (DMCA)," *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>

⁷⁸ Samuelson Law, "Frequently Asked Questions (and Answers) about Anticircumvention (DMCA)," *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>

⁷⁹ Samuelson Law, "Frequently Asked Questions (and Answers) about Anticircumvention (DMCA)," *Chilling Effects*, <http://www.chillingeffects.org/anticircumvention/faq>

⁸⁰ "Frequently Asked Questions (and Answers) About the Dmitry Sklyarov & ElcomSoft Prosecution," Electronic Frontier Foundation, http://w2.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html

⁸¹ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁸² Sara Baase, *A Gift of Fire, 2nd Edition* (London: Pearson Education, 2003), Page 259

⁸³ Siva Vaidhyanathan, *The Anarchist in the Library* (New York: Basic Books, 2004), Pages 90 – 91

⁸⁴ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁸⁵ Cory Doctorow, "Microsoft Research DRM Talk," *Electronic Frontier Foundation*, Hosted by Dashes.com, <http://www.dashes.com/ani/stuff/doctorow-drm-ms.html>

⁸⁶ Steve Jobs, "Thoughts on Music," *Apple.com*, <http://www.apple.com/hotnews/thoughtsonmusic/>

⁸⁷ Sir Timothy Berners-Lee, "Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act," *Cato Institute*, http://www.cato.org/pub_display.php?pub_id=6025