Piracy in the Digital Age

Dana Dahlstrom, Nathan Farrington, Daniel Gobera, Ryan Roemer, Nabil Schear
University of California, San Diego

CSE 291 (D00) – History of Computing

December 6, 2006

I. Introduction

Copyright owners are at no loss for words and figures asserting the detrimental effects of unauthorized copying and distribution of software and digital media. The recording industry estimates present worldwide losses at $4.2 billion per year.[1] The motion picture industry puts 2005 worldwide losses at $18.2 billion,[2] and the software industry claims a $34 billion figure.[3] Put together, the estimated losses from piracy in these three industries in 2005 exceed the approximately $50 billion in worldwide damages from all the spam sent that year.[4] Even taken with the proverbial "grain of salt," these estimates provide at least a crude indication of a large and growing phenomenon.

The term "piracy," as used in this paper, refers to the illegal copying and distribution of proprietary content such as software, music, or movies. Some unauthorized copies are "bootlegged," copied for later resale at below-market prices. Other unauthorized copies are made and distributed by consumers who trade them without payment. In a break from traditional notions of piracy and counterfeiting, the "digital piracy" of primary concern today involves non-physical objects: digital files sold or exchanged over the Internet.

Mode and motivation aside, the extent of piracy is most frequently measured in monetary terms: the revenues that might otherwise have resulted from the authorized sale of the goods that were illegally copied instead. One can question the assumptions underlying loss estimates: Would all "pirates" otherwise have purchased all the same goods at full price? At the same time, might not unauthorized copies sometimes expose people to content they decide to purchase, thereby actually producing sales? Despite the likely answers to these questions, the content industry primarily perceives "piracy" as a threat to their business models; undoubtedly others perceive great opportunity. Accordingly, the content industry has gone to great lengths technologically, politically, and legally to stem the tide of unauthorized copying and distribution facilitated by the Internet and other technological advances.

This paper will explore the history of the primary forces driving digital piracy: improving technology that makes it faster, cheaper, and easier for more and more people to copy and distribute exact digital copies of proprietary content. Many of the modern day issues with piracy can be traced back to the early history of computing. The availability of widespread digital distribution and massive storage has inflated previously unimportant aspects of piracy into large controversial issues. Technological advances also allow improved content protection and digital rights management. However, most advances in content protection are met with technological "hacks" or "cracks" that create an escalating "arms race" scenario. As intellectual property owners seek stronger legal protection against piracy, new laws and legal doctrines similarly find that technology can even circumvent

[1] RIAA, *Anti-Piracy Issues*, *available at* http://www.riaa.com/issues/piracy/default.asp (last visited Dec. 5, 2006).
[2] MPAA, *Who Piracy Hurts*, *available at* http://www.mpaa.org/piracy_WhoPiracyHurts.asp (last visited Dec. 5, 2006).
[3] Press Release, *Piracy Rate Unchanged at 35%; Global Losses Increased by $1.6 Billion*, BSA (May 23, 2006), *available at* http://www.bsa.org/EastMediterranean/press/newsreleases/eastmediterraneanpressrelease23may2006.cfm.
[4] Gregg Keizer, *Spam Costs Businesses Worldwide $50 Billion*, INFORMATIONWEEK (Feb. 23, 2005), *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=60403016.

legal rules, and leave an imperfect (and possibly harmful) intellectual property framework.

This paper begins with a discussion of media piracy in Section II, examining the incidence and motivation for media piracy, tracing the historical development of various media technologies into the digital age, and noting the technologies that facilitate and fight digital media piracy. Section III explores the development of software as an independently valuable product, copying and distribution of software, and technological software "locks" used to enforce copy protection. Section IV examines the evolution of traditional civil and criminal copyright law in response to the rise of file sharing networks, and looks at the impact of the Digital Millennium Copyright Act on digital "lock picking" software and research generally.

Finally, this paper concludes with the assessment that the underlying technological and social factors behind digital piracy will likely ensure that piracy will continue to be an escalating sociopolitical controversy and problem for copyright owners. In many respects, the technological capabilities enabling piracy outpace the legal and other means to stop them. The controversy, it seems, is likely only to expand.

II. Media Piracy

A. Introduction

1. Digital Media, Piracy and Technical Background

To begin with, the phrase "digital media" will be used to refer to data that can be represented and stored electronically, encoded in a binary format, and suitable for interpretation by modern computers. The type of data is unbound, but for practical purposes it will be assumed that it is typically multimedia content encompassing text, images, music, and video. As opposed to content stored in physical media, such as books and paintings, digital content has the special quality of being extremely easy to reproduce. And as opposed to analog content stored on magnetic media, which is also easy to reproduce, it does not lose quality when duplicated. The information is represented numerically, so merely copying this sequence of numbers results in an exact and undistinguishable copy of the original.

This easiness of reproduction is both a virtue and a drawback of this kind of technology. It dramatically reduces production times and costs, and enables new distribution channels, like online media stores, in addition to the traditional physical discs or cassettes. On the other side, it brings a whole new world of possibilities for duplicating and distributing content without the required authorization. Machines capable of creating thousands of exact copies of a compact disc or computer networks that can transfer a movie in minutes are just some examples.

Media piracy is the act of reproducing and/or distributing protected content without previous authorization from the copyright holder, usually for a personal benefit. Due to the reasons explained above, such as the ability to create perfect copies, the rise of media in digital format has significantly aggravated the problem. As an example, a report from the IFPI stated that the explosion of CD-Rs in Mexico took the piracy rate from 45% to 63% in 2001.[5] Content creators have found themselves in need of protecting their intellectual property in any manner possible. The two most common mechanisms, and the ones examined in this paper, are legal and technical: copyright legislation and digital locks.

In the United States, copyright law provides the most widely used intellectual property legal protection for digital media. As discussed further below in Section IV of this paper, the Copyright Act provides protection for musical, pictorial, and audiovisual works, as well as motion pictures and sound recordings. Anyone who violates

[5] Adrian Strain, *Piracy threatens future of music industry in Mexico*, IFPI (May 17, 2001), *at* http://www.ifpi.org/content/section_news/20010517.html.

the exclusive rights of copyright (by copying, distributing, etc.) without authorization or excuse is liable for copyright infringement.

Digital media locks are the technological means for content creators to prevent unauthorized copying or use of the material, even when the infringer has decided to overlook the laws preventing this. There are a large number of these mechanisms, so this paper will concentrate on the most popular and influential ones. In most cases, they are artificial restrictions that had to be added to media that is inherently readable and reproducible by standard electronics and computers. As a result, it is often a matter of time before a way to circumvent them is discovered, as discussed in the following sections.

2. Motivations and Consequences

The issue of digital media piracy can be regarded differently from the point of view of each of the involved parties. In most cases, we can discern three roles: the content creator or distributor, who can perceive a loss (monetary or of another kind) from the piracy act, the "pirate," who can make a profit from illegally copying and distributing the protected material, and the end consumer, who ultimately decides to which of the previous two parties his money goes.

From the creator/distributor perspective, piracy is a direct harm that needs to be eliminated. Record labels, movie studios, and other organizations lose a considerable amount of money each year due to media piracy. The RIAA reported $4.2 billion in losses worldwide[6] last year, with the MPAA reporting $18.2 billion[7]. These numbers can sometimes be misleading, because the studies often speculate that a large percentage, if not all, of the consumers that acquired an illegal copy would otherwise have bought an original one. This is not the case for most underdeveloped countries where the average income makes it prohibitive for most to afford an original album or movie. In any case, these figures are alarming enough for the companies to invest significant resources into developing locking mechanisms to prevent the illegal reproduction of the material.

Turning now to the other side, we find that people who illegally copy and distribute media, often called "pirates," normally have an economic incentive to do it. They need only one copy of the material to create thousands of copies to be sold at extremely low prices compared to the original. This copy can be obtained by legally buying it or by other, often illegal, means with even lower cost (*e.g.*, another illegal copy, a robbed original copy, or recording a movie in a theater with a video camera). The price of the physical media to distribute the copies is almost negligible; for example, blank compact discs can be bought in mass for less than a dime apiece. And as the cost of the machinery needed for duplication is also constantly dropping, piracy can be a very profitable business. Media pirates are willing to take the risk of facing legal charges, and are constantly investing considerable resources in finding ways to circumvent media locks. A curious phenomenon is that these "intermediaries" are less and less needed by the whole piracy mechanism, since it is now possible for consumers to create their own copies and share them directly, without the need of specialized machinery.

The third role, consumers, represents the target for the other two. They are ultimately who will spend money acquiring the media and often have the option of buying the original or somehow get a pirated copy. The first one has many benefits, like quality standards, packaging, extras (like booklets or secondary discs), peace of mind, and, more importantly, legality. But the reason why piracy exists is that the second option provides a very tempting deal: a nearly-as-good product for a ridiculously lower price.

---

[6] RIAA, *Anti-Piracy Issues*, *at* http://www.riaa.com/issues/piracy/default.asp (last visited Dec. 5, 2006).
[7] MPAA, *2005 U.S. Piracy Fact Sheet*, *at* http://www.mpaa.org/USPiracyFactSheet.pdf (last visited Dec. 6, 2006).

B. The Beginnings of Media Piracy

1. Early History

This ability to quickly and cheaply produce essentially perfect copies is relatively recent development. Technologies for different forms of content — text, images, and sound and video recordings — have taken somewhat different courses, but we can identify some general patterns. The first technologies used analog representations in physical or mechanical media, followed by analog representations in magnetic media, and finally digital representations that are largely medium-independent. At each stage, the newest technology was first made available to and affordable only by those in the business of producing and distributing content, and subsequently became less expensive and more widespread. The means of production, reproduction, and distribution became easier, cheaper, faster, and more widely available; and the results of higher quality.

Text, the visual representation of language, is the form of content with the longest history. For thousands of years before the advent of the movable-type printing press, in Asia in the 13th century C.E. and in Europe in the 15th, the only way to copy text was by hand. This was slow and expensive, and access to written work was therefore so limited that the unauthorized making or distribution of copies could hardly have been conceivable, let alone viable. Even the printing press did not raise this issue right away, because the cost to purchase and operate the machinery was a significant barrier to those who might otherwise have sought to undercut publishers. The legal concept of copyright for literary works did not arise in Europe until the 18th century.

2. 20th Century

It was not until the 19th century that photography made it possible to automatically produce images. The first photographs were made in the 1820s; the materials, processes, and equipment evolved continually thereafter, leading eventually to the mass-market film cameras and color photography of the 20th century. While still photography was developing, sound recording got its start in the 1850s with "phonautograph" devices that recorded images of sound waves, leading to "gramophones" and "phonographs" that could reproduce sound in the 1880s. In the same decade, the first motion-picture cameras enabled what we would later come to call video recording.

All the technologies mentioned so far were mature by the turn of the 20th century. All were based on physical, mechanical, or chemical processes that did not enable easy duplication of the artifacts they produced. And except in the case of still photography, the technologies were complex and expensive enough to limit the content-bearing artifacts — books, records, and motion pictures — to centralized production and commercial distribution.

Recording sound magnetically became practical in the 1920s, once it was possible to amplify weak electrical signals with good fidelity. The first magnetic sound-recording medium was metal wire, followed by metal tape, and later by paper and eventually plastic tapes coated with metallic powders. Magnetic recordings were important not only because they were easier to duplicate, but also because the linear medium enabled its users to edit by cutting and splicing, and the technology was widely used in the burgeoning radio-broadcasting industry.

Electrophotography, first discovered in the 1930s, led to the commercialization of "Xerography" (literally "dry writing") in the 1940s. The company Xerox took its name from the process, later generically called "photocopying" so as not to weaken Xerox's trademarks. With a photocopier, one could make reasonably good paper replicas of black-and-white text or images; color photocopiers followed eventually in the 1980s.

Motion pictures, or "movies," had no sound at the turn of the 20th century, apart perhaps from a live accompanist. In the 1920s, enabled again by magnetic recording and electrical amplification, filmmakers began to release motion pictures with synchronized movie soundtracks including music, speech, and effects. Magnetic

recording of video essentially coincided with popular television broadcasting in the 1950s, where it was used in professional studios.

Equipment that could play and record audio on magnetic tape was widely available to consumers in the 1960s, but the release of home videocassette recorders in the 1970s prompted a legal challenge that would take nearly a decade to resolve and would set wide-reaching precedent affecting the commercialization and use of later technologies. VCRs allowed people to record television broadcasts to which the studios owned copyrights. Recognizing that it would be infeasible to pursue each infringing VCR owner, the studios instead sued the manufacturer. The ensuing lawsuit, *Sony v. Universal*, is discussed in Section IV below.

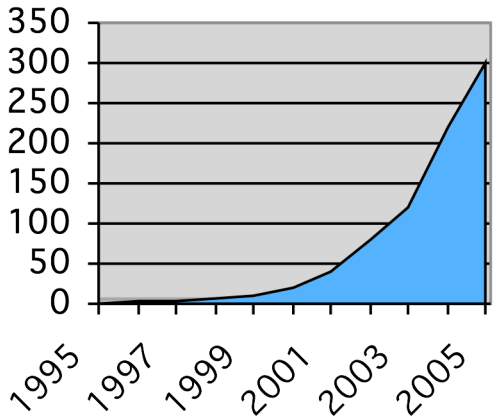
The 1980s saw the first popular medium for distributing digitally encoded content to consumers: the compact disc. Though the century-old phonographic disc had dominated this market for most of its existence, the CD would make it obsolete by the end of the decade. But this was only the beginning of the changes brought about by the popularization of digital media.

C. Recent History

1. Media Formats and Compression

Until recently, digital music and video could be stored and transported only in specialized high-capacity media, like tape, CDs and DVDs, due to the large amount of space they needed. As an example, a four-minute song with CD quality uses about 40 MB, and the average hard drive capacity in the late 1990s was about 1 GB, making it impractical to store more than a few songs there. Also, the average Internet connection at that time was via 56 kbps modems, which would take more than two hours to transmit the mentioned song.[8]

As technology advances, these restrictions have become less and less relevant. Storage capacity of current hard drives is typically measured in the hundreds of gigabytes, and in mid 2006 almost half of the American population had broadband Internet access.[9]



Evolution of capacity of typical hard drive in personal computers in GB.

But the key advance to make media manageable in personal computers has been the evolution of data

[8] *Cost of Hard Drive Storage Space*, *at* http://www.alts.net/ns1625/winchest.html (last visited Dec. 6, 2006).
[9] John Horrigan, *Home Broadband Adoption 2006*, PEW Internet (May 28, 2006), *available at* http://www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf.

compression algorithms, called codecs, which can considerably reduce the size of media files. The MPEG-1 Audio Layer 3 format, or MP3, was developed in Germany as part of the EUREKA European research project, and became part of the MPEG-1 standard in 1991. This encoding/decoding algorithm can compress audio files to about 1/10th of the original size in uncompressed CD format. Being a lossy algorithm, some of the original data is lost during the compressions process, but the end result has good enough quality for most listeners. The previously mentioned four-minute song with compression would use about 4 MB. This file could then be transferred in less than 10 seconds over a broadband Internet connection, a 720 times improvement over late 1990s technology. The MP3 audio format did not become popular until after 1995, when the Fraunhofer Society released the first software encoder and the first player applications became available. Many other similar compression algorithms followed the MP3, like MPEG-4 AAC, Ogg Vorbis, and Windows Media Audio. But due to the high popularity of MP3, it has become the generic term among consumers to refer to all these kinds of encoders.[10]

Image and video compression has followed a similar path. New encoding technologies have significantly reduced the file sizes, making it possible to store and share images and video through conventional computers and networks. PNG and JPEG are two of the most popular formats for images. For video, some of the codecs include MPEG-2 (used for DVDs and television broadcast), DivX, Windows Media Video, Sorenson 3, and the MPEG-4 family of standards, including the recent H.264/AVC. This last one is the format of choice for many portable video devices and high definition discs, due to its considerable compression ratio and low quality loss (about 11 MB per minute of near-TV quality video).[11]

2. Media Sharing

The increasing capacity for storing and transferring digital media files on computers and networks has opened new opportunities for content creators, distributors, consumers, and of course, pirates. Soon after the release of the MP3 codec, people began to rip music they owned from CDs to MP3 files on the hard drive. MP3 files are small enough to transfer via Internet connections, so users started sharing music using many different kinds of services, like FTP, Web pages, IRC and even e-mail. As the original CD designers did not anticipate this scenario, tracks on a compact disc are unencrypted and lack any content protection mechanism. At this point in time, the law regarding shifting media formats to digital was quite undeveloped.

Peer-to-peer networks turned out to be an excellent match for the kind of activity music sharing users needed, and are often called "file sharing networks" when used for this purpose. This kind of computer network has the characteristic of requiring only a few servers (or none at all) because participants send information directly to each other. Peer-to-peer networks have been around since the early 1980s, with Usenet being one of the first. New file sharing services specializing in music sharing emerged, such as Napster, Gnutella, FastTrack, Entropy, eDonkey, and many others. These services relied on a few servers to facilitate finding other users and sometimes maintaining a search index of the available content on peers. They also encourage users to share their files by providing incentives (like download bandwidth limited by amount of files shared) or by automatically making all downloaded files available for sharing.[12]

Napster was the first of these services to become popular. It started in 1999, and by 2001, it had more than 10 million users. Its central servers maintained a list of connected users, as well as an index of all files shared by all

[10] Fraunhofer-Institut für Integrierte Schaltungen IIS, *MP3: MPEG Audio Layer-3*, *at* http://www.iis.fraunhofer.de/amm/techinf/layer3/ (last visited Dec. 6, 2006).
[11] Leonardo Chiariglione, *The MPEG Home Page*, *at* http://www.chiariglione.org/mpeg/ (last visited Dec. 6, 2006).
[12] Stephanos Androutsellis-Theotokis and Diomidis Spinellis, *A survey of peer-to-peer content distribution technologies* (2004), 36 ACM Comput. Surv. 335-371.

peers for quick search. It quickly became the most popular way for many people to get new music, which became essentially free. As its popularity continued growing, it started to draw the attention of artists, record labels, and of course, the Recording Industry Association of America. It was sued several times over the argument that it was promoting illegal distribution of copyrighted material, which had a direct effect in record sales. On July 2001 Napster was shut down, but several other file sharing networks continued to be operational.

D. Media Content Protection and Digital Rights Management

The entertainment industry learned an important lesson from this whole phenomenon: copyright laws are not enough to stop piracy; mechanisms are needed to physically impede the unauthorized reproduction of digital content. Companies have also realized that the Internet can be a good medium of content distribution, but have been very cautious in exploring this market without the appropriate protection mechanisms.

Digital Rights Management, or DRM, refers to a variety of technologies that allow content creators and distributors to control how the media is used and copied. DRM schemes typically combine techniques like encryption and user authentication, and rely on features of electronic media players. A good example of DRM is the "Content Scrambling System," or CSS, which has been used to protect DVDs since the mid-1990s. CSS uses a simple encryption algorithm to prevent the disc contents from being read by unauthorized equipment, particularly duplication tools. Like many other protection schemes, it was susceptible to attacks. In 1999, CSS was reverse-engineered by a teenager, Jon Lech Johansen, who released a tool called DeCSS to circumvent the rights management mechanism.[13]

Online music and video stores have recently emerged, selling individual songs or entire albums in MP3 or similar format. The current market leader, the iTunes Store, uses a somewhat restrictive and controversial DRM scheme. iTunes DRM format, FairPlay, is built into QuickTime technology and uses encryption to prevent unauthorized playing of the content. At the moment of purchase, every song and video is bound to a particular account. The user is allowed to play the file in up to five computers and an unlimited number of iPods. It has been the object of multiple complains and even lawsuits from competitors that want to be able to either make their protection schemes work on the iPod or make FairPlay-protected songs playable in devices other than the iPod. The protection mechanism has been successfully reversed-engineered a number of times, initially by Johansen. Apple has responded with legal warnings and by continuously updating its software to disable any new workarounds. Other popular DRM systems, like Microsoft PlaysForSure, RealNetworks Helix, and Zune DRM, impose similar restrictions on the media and face similar problems.[14]

A more controversial DRM technology is the so-called "Sony Rootkit." Realizing that music in CDs is not protected by any technical means, Sony incorporated MediaMax and XCP software in some discs sold during 2005 to prevent ripping and duplication of the material on personal computers. The problem is that this software interferes with the normal operation of the operating system, is installed without notifying the user, and there is no uninstaller. It was also found that it could open security holes in the system, posing a risk to legitimate buyers. The software was classified as "spyware," and several lawsuits were filed against Sony, who had no choice other than recalling the affected CDs.[15]

---

[13] *See* DVD Copy Control Association, *Content Scramble System (CSS)*, (2006), *at* http://www.dvdcca.org/css/ (last visited Dec. 6, 2006); *see also* DeCSS Central, *CSS and DeCSS*, *at* http://www.lemuria.org/DeCSS/decss.html (last visited Dec. 6, 2006).

[14] *See, e.g.*, Apple Computer, *iTunes Customer Service – Computer Authorisation*, *at* http://www.apple.com/lu/support/itunes/authorization.html (last visited Dec. 6, 2006); Liz Gannes, *DVD Jon Fairplays Apple*, GigaOM (Oct. 2, 2006), *at* http://gigaom.com/2006/10/02/dvd-jon-fairplays-apple/.

[15] *Anti-Piracy CD problems vex Sony*, BBC News (Dec. 8, 2005), *at* http://news.bbc.co.uk/1/hi/technology/4511042.stm; Mark Russinovich,

E. Lessons from Digital Media Locks

Although media distributors consider digital rights management a necessity to fight piracy, it sometimes gets in the way of legitimate consumers by restricting the use they can make of material they legally buy and own. Complaints range from simple annoyances, like having to authenticate as a user to play purchased music, to more serious problems, like not being able to play the media due to incompatibilities or errors in the protection mechanism. There are a number of movements that object to DRM and argue it limits consumer rights and information access. Major opponents include John Walker, Richard Stallman, and Ross Anderson, along with organizations like the Free Software Foundation, the Electronic Frontier Foundation, FreeCulture.com, and the Foundation for a Free Information Infrastructure.

As we can conclude, protection of digital media is a very difficult problem. This kind of media is inherently easy to read and reproduce by electronic means, so all protection mechanisms are artificial limitations that rely on features on the player devices. Software-based DRM mechanisms have an inherent flaw; as the "Defective by Design" anti-DRM campaign puts it: "DRM is a technical problem, and can be solved by technical means. This was true five years ago—all DRM was ultimately software, all software is data, and all data is mutable. So, DRM could always be circumvented."[16] DRM developers are experimenting with new hardware-based alternatives, usually enforced by firmware. These new alternatives promise a much harder to break mechanism, but pirates, hackers and DRM opponents will invest all their efforts into finding ways to circumvent them, and will likely be successful sooner or later.

III. Software Piracy

A. Origins of Software and Rise of Piracy

As we have seen with media, sharing content has a history as old as methods to store and duplicate it. Text in books was not readily copied until well after the printing press was invented. Similarly, images could not be shared until photograph and subsequent technologies were invented. Digital media was simply an explosion of an existing phenomenon while computer software was born *with* this digital revolution. For this reason and others we discuss below, the history of software piracy has been divergent from that of traditional media piracy. This trend between software and media piracy has converged, but only within the last ten years.

In the early days of computing, ownership of anything "digital" was something of an open question. In the 1970s, many believed software, for example, was something to be shared, collectively used, and improved. Even earlier, software was barely regarded as having independent worth at all. Thus our discussion of the origins of software piracy begins with the history of the software's emergence as a product apart from hardware and establishment as an industry in its own right, conferring clear, monetary value on a purely "digital" entity.

1. Software Origins and Value

At the advent of the computing age software and hardware were inseparable. For example, ENIAC's software was "encoded" in the cable connections made by its operators. UNIVAC and IBM were the first to productize computers and both sold an all-in-one system. This included the hardware itself, software (sometimes custom developed), and onsite support. This product model continued for most computer companies well into the 1970s.

Sony, Rootkits and Digital Rights Management Gone Too Far, Mark's Blog (Oct. 31, 2005), *at* http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx; F-Secure, *F-Secure Computer Rootkit Information: XCP DRM Software*, *at* http://www.f-secure.com/v-descs/xcp_drm.shtml (last updated Nov. 30, 2005).

[16] *About Defective By Design*, DefectiveByDesign.org, *at* http://www.defectivebydesign.org/en/about (last visited Dec. 6, 2006).

Partially in response to the Justice Department's anti-trust inquiries, IBM offered unbundled software as a separate product in 1969.[17] This event is largely credited for creating a viable and profitable software business.[18] Nonetheless, IBM continued to sell software and hardware together as one package for many years. Though software companies existed before this, they primarily sold custom made software for very specialized purposes. It took many years for software to come into its own as an independent product. Computer programs were not defined in US copyright law until the Computer Software Copyright Act of 1980 and not fully protected until *Apple v. Franklin* in 1983.

a. Software Becomes Valuable

Once it became a separate product, the value of software began to increase. Software had a very different model of development from hardware because the first copy constituted most of the cost. It became valuable only when it could be sold in large volume amortizing this high up front cost across many copies. Mainframe software was often included with the purchase of the hardware. The only custom software applications at the time (*e.g.*, airline booking, custom databases) were developed for a very small set of customers.

Though a major player in the computer business, DEC did not invest heavily in the software for their computers, thinking it unprofitable. This led to software businesses built around their PDP and VAX mini-computers.[19] These companies were never wildly successful, but they were able to subsist primarily because DEC chose not to participate.

As computer hardware continued to become smaller and less expensive, large volumes were achieved and software became very profitable. For example, at its peak, VISIcalc yielded Software Arts 12 million dollars in royalty profits in 1981.[20] BASIC for the Altair was Microsoft's first product and provided the start for the company to enter the operating system market with the IBM PC.

b. Customers

The world has slowly moved through a number of computer classes as specified by Gordon Bell.[21] Each time a new computer class emerged, the number of nature of the customers of the computer industry changed. The military was the first customer of the computer. Customers then expanded to include large companies and some academic institutions with mainframes. Next, computers became available to medium sized businesses and more in the research community with mini-computers. Up until this point, individuals rarely owned computers. Personal computers changed that trend and opened the computer to a large and varied audience. Lastly, the Internet made computing accessible to a huge worldwide audience. Now that software had a sufficiently sized and varied customer base and had become valuable, software was ripe for copying and piracy.

2. Software Copying and Sharing Early-History

Since early computer companies were primarily interested in selling the hardware, users banded together to enhance their software. A group of IBM 701 users started the SHARE user group in 1955.[22] SHARE members

[17] Robert Parker and Bruce Grimm, *Recognition of Business and Government Expenditures for Software as Investment: Methodology and Quantitative Impacts, 1959-98*, report presented at the meeting of the Bureau of Economic Analysis, (May 5, 2000), *available at* http://www.bea.doc.gov/bea/papers/software.pdf.
[18] B. Grad, *A personal recollection: IBM's unbundling of software and services*, 24 ANNALS OF THE HISTORY OF COMPUTING (2002), IEEE 64-71.
[19] C. G. Bell, *The Mini and Micro Industries*, 17 COMPUTER 14-30 (Oct. 1984).
[20] Tom Hormby, *VisiCalc and the Rise of the Apple II*, Low End Mac (Sept. 25, 2006), *at* http://lowendmac.com/orchard/06/0922.html.
[21] C. G. Bell et al., *A New Architecture for Mini-Computers -- The DEC PDP-11*, Sprint Joint Computer Conference (1970), pp. 657-675.
[22] Mary Brandel, *1955: IBM customers form the first computer user group*, CNN (May 5, 1999), *available at* http://www.cnn.com/TECH/computing/9905/05/1955.idg/index.html.

traded and developed software for IBM products. This group ended up being very helpful to IBM because it increased the usefulness of their hardware with better software. Later, similar software user groups formed around DEC computers.[23]

a. Open vs. Close Source

Most hardware manufacturers up until the 1980s had a very open approach to software. The earliest versions of IBM software were distributed in source form.[24] When software became more valuable this trend reversed quickly as it became obvious how much money was to be made. Contrary to this trend Richard Stallman started the GNU project for a free operating system in 1983.[25] Berkeley also developed a version of UNIX during the 1980s, which was released under an open source license.

Today Linux and other open source projects are gaining acceptance and adoption by large computer corporations. Because the software itself is freely available when it is open source, the problem of piracy disappears. Many companies *are* profitable selling service and support for open source software. However, closed source proprietary software still dominates the industry. We do not intend to discuss the whether open source software is the solution, but only to highlight its effect on piracy.

3. PC Software

The PC brought computers to a much larger audience than ever before. The computer became a tool for businesses and home users alike. In the late 1970s, the PC market was dominated by hobbyists who liked "tinkering." Microsoft BASIC for the Altair (an early hobbyist computer) was very successful as it was one of the first applications for the fledgling PC market. At this time, BASIC was distributed on paper tapes, which were difficult, but possible to copy. In one of the first public acknowledgements of the problem of piracy, Bill Gates wrote to hobbyists, "most of you steal your software."[26] Gates went on to say that software would not be a sustainable business if people continued illegal sharing. Gates remarks were in response to widespread illegal copying of BASIC and use of a stolen development release.[27]

a. Sharing Floppies in the 1980s

Floppy disk drives became the *de facto* standard for file storage and distribution in the early 1980s. Many computers of this time were used for game playing. Users would share floppy disks of popular games with friends and often copy them. To prevent this, software companies started implementing protection schemes and locks. We will discuss some of these methods in Section III.B.

It was during this time that software businesses started to take notice, and two organizations were formed: the SPA (Software Publishers Association, est. 1984, now known as the Software & Information Industry Association) and the BSA (Business Software Alliance, est. 1988). Both organizations aim to protect copyrighted software from illegal copying. In 1992, the SPA launched a campaign titled "Don't Copy That Floppy," which was designed to educate users against illegal copying and its potential decrease the number and quality of computer games.[28]

---

[23] Edgar H. Schein et al., DEC IS DEAD, LONG LIVE DEC: THE LASTING LEGACY OF DIGITAL EQUIPMENT CORPORATION (2003).
[24] Wikipedia, *SHARE*, *at* http://en.wikipedia.org/wiki/SHARE_(computing) (last visited Dec. 6, 2006).
[25] Richard Stallman, *The GNU Project*, *in* OPEN SOURCES. VOICES FROM THE OPEN SOURCE REVOLUTION (O'Reilly & Associates, 1999).
[26] Bill Gates, *An Open Letter to Hobbyists*, Homebrew Computer Club Newsletter (Feb. 3, 1976), *available at* http://www.digibarn.com/collections/newsletters/homebrew/V2_01/gatesletter.html.
[27] Paul Ceruzzi, A HISTORY OF MODERN COMPUTING (2003).
[28] Wikipedia, *Don't Copy That Floppy*, *at* http://en.wikipedia.org/wiki/Don't_Copy_That_Floppy (last visited Dec. 6, 2006).

4. Networked Computers and Piracy

a. Bulletin Board Systems (BBS)

Though the DARPA Internet was in use, Bulletin Board Systems ("BBS") dominated internetworking in the 1980s and early 1990s. Their ease of access and community atmosphere created an ideal forum for sharing of any kind of information. Affordable PCs and increasingly faster modems made BBSes more suitable for software distribution. Shareware (*i.e.*, software that is free to try but must be purchased for extended use) was first distributed through BBSes. Many BBS users traded software, games, and shareware (collectively known as "warez") for various PC platforms through the 1980s.

Eventually, there were BBS sites devoted entirely to sharing pirated software. Since a BBS is inherently a local service to which users dial-in, gaining access to a remote BBS required an expensive long-distance phone call. In the late 1980s, BBS software pirates and phone "phreakers" teamed up to "courier" software to and from remote sites by making free phone calls using tone generating blue-boxes.[29] Hosting pirated content freely (*e.g.*, David LaMacchia at MIT) was not a crime in noncommercial situations before the Net Act.[30] Since for-profit software piracy was illegal both civilly and criminally during this time, many BBSes were at risk for prosecution because they had monthly access charges. Most BBS sites were hosted from the system operator's home, so it was easy to locate the owner and potentially prosecute them.

The use of BBSes for software piracy came to end as the Internet gained dominance. Its end was also predicated by the FBI's Cyber Strike crack down on warez-oriented BBS sites in 1997.[31] Many groups in the BBS warez scene moved their operations to the Internet using Usenet and IRC.

b. The Internet and Widespread Warez

The Internet had a profound effect on communication and information sharing on a global scale. Software piracy also relieved users from needing a courier to move files from remote BBSes. It also opened nearly any Internet user to what was once a very underground secret.

(i) IRC and Usenet

Though some in the BBS software warez scene disparaged it, Internet relay chat (IRC) channels became one of the most prevalent methods for distributing pirated software. Warez groups communicated extensively with each other using IRC. It followed that they could use XDSS (a protocol for IRC users to exchange data directly) to distribute software. At first, IRC channels were closed to external users and the closed environment built up during the BBS era remained. A naïve user wanting to access pirated software would have to gain access to the IRC channel, most likely by getting help from an existing member. Eventually, many IRC channels were opened to the public. Some new users found IRC to have a steep learning curve for general use; however, collecting software was as easy as browsing a file system to locate pirated content.

Another important venue for pirated software was Usenet. Usenet is an Internet-based bulletin board system started in 1979.[32] It was originally conceived to allow users to exchange text content within newsgroups of a certain topic. Because of its inherent text medium, users must encode binary content (like software and media) into the 7-bit ASCII format. Usenet posts also often have a maximum size causing users to split large files across many

---

[29] Ben Garrett, *Online Software Piracy of the Last Millennium* (Apr. 27, 2004), *at* http://www.defacto2.net/documents.cfm?id=183.
[30] Jeremy Hylton, *David LaMacchia cleared; case raises civil liberties issues*, THE TECH (Feb. 7, 1995), *at* http://www-tech.mit.edu/V115/N0/lamacchia.00n.html.
[31] *FBI hunts software pirates*, CNET News.com (Jan. 28, 1997), *at* http://news.com.com/FBI+hunts+software+pirates/2100-1023_3-265813.html.
[32] *See* Wikipedia, *Usenet*, *at* http://en.wikipedia.org/wiki/Usenet.

posts. Binary content though rare on Usenet initially now constitutes over 90% of all Usenet traffic[33] and many companies now sell subscriptions to access Usenet binaries for a monthly fee.[34]

When the availability of broadband access became more prevalent in the late 1990s, larger games and applications could easily be distributed. The sizes of software distributions caused those who created and released pirated software to standardize. They even went so far as to form standards organizations like the Standards of Piracy Association (SPA, an acronymic pun on the anti-piracy Software Publishers Alliance). The piracy SPA formed out of the largest warez groups and their standards defined file formats and sizes, and attempted to regulate releases of pirated software. The SPA eventually dissolved and other powerful groups attempted to enforce commonality between pirated releases. Though most of the organizations formed to enforce these standards eventually failed because of bickering between the members (as often happens in standards committees), the effect of the standards was very powerful and affects pirated software releases to this day.

(ii) Web Hosted

As the "killer-app" of the Internet, the World Wide Web was heavily used to traffic pirated software. Warez groups on IRC and Usenet that favored openness eventually created web sites to host the software. These sites provided new users with a first glimpse into the warez scene. Many sites also contained guides and FAQs for finding pirated software through more advanced methods like IRC.

Similar to BBS sites, web sites operators are easy to locate by law enforcement because the site must eventually lead to a server and Internet connection. Many sites were hosted directly in less developed countries without piracy law like those in Eastern Europe and Southeast Asia. Since many warez groups were located in first world nations with increasingly strict laws, they found ways to not store the pirated software directly but only *link* to it. However, some countries, such as the United States, have even made indexing (or linking) the locations of copyrighted content illegal, as discussed further in Section IV. Sites created during the Internet bubble to provide free online storage, like I-Drive and Driveway, were often used to host pirated software.[35] Many of the storage sites responded by trying to limit bandwidth. Eventually, web hosted warez lost favor because of the ease of attribution. Though many sites only posted links to sites like I-Drive with pirated content, many had civil legal actions brought against them and were forced to shut down.

(iii) P2P Networks

As discussed previously, peer-to-peer ("P2P") networks were first used to distribute music, images, and video. After the success of Napster for music, some P2P networks also began hosting software. Due to legal problems with direct Web hosting, the distributed nature of P2P systems provided a safer alternative. P2P networks opened piracy to a much larger audience. The interface was easy and did not require extensive background knowledge or jargon, as was the case with other methods. Though pirated software is not often targeted for legal action against P2P users or systems the way it is for media, it still accounts for a large volume of the data.

The latest P2P technology to influence piracy is BitTorrent. BitTorrent allows users to share content by only communicating with each other so there is no central control that can be legally or otherwise targeted. A central facet of P2P networks is the need for all peers to participate in uploading content to other peers rather than just greedily downloading only. BitTorrent and other systems have tracking methods to ensure that all users are participating. Recent research has shown ways to bypass the upload tracking methods in BitTorrent and could bring

[33] *Binary News*, Usenet.com, *at* http://www.usenet.com/articles/binary_news.htm (last visited Dec. 6, 2006).
[34] *See, e.g.*, Easynews website *at* http://www.easynews.com/ and Newsreader.com website *at* http://newsreader.com/.
[35] Richard Spann, *Black Warez: Software Piracy and Internet Distribution* (Dec. 7, 2000), at http://www.dawnsky.com/raspdf/blackwarez.pdf.

BitTorrent down if enough users want to be greedy.[36]

Web hosting, Usenet, and other P2P systems make pirated content freely available to any user who wants to access it. The architecture of BitTorrent allows sharers to form private communities mimicking the underground culture of BBSes and IRC.[37]

c. Security

The line between those who crack software and those who hack into others' computer systems has always been very fine. The BSA asserts that most pirated software is infected with malware and Trojan horse programs. Recent studies confirm this fact for peer-to-peer systems like Kazaa and Limewire. The studies found that between 15-68% of all archive and executable content on select P2P systems contained viruses and other malware.[38] Because of P2P system's global connectivity and millions of users, it is unclear whether malware writers are targeting the pirated software or the P2P systems themselves. Unfortunately, it is difficult to track other distribution mechanisms for dangerous software, and thus the BSA's claims are difficult to validate.

5. The Future of Pirated Software

Software piracy continues to be a problem especially outside the United States. For example, it has become common in Asia to find shrink-wrapped pirated software available through retail vendors.[39] Some clerics of Islam have also condemned piracy (only under certain conditions); however, piracy remains common in Muslim countries.[40] As discussed previously, according to the BSA, it already cost the software industry $34 billion in 2005.

The future of the software industry will inevitably include dealing with piracy. If software is valuable, people will find a way to share it. Since the digital medium makes copying so easy, the damage done to the creator of the software is less tangible to the end user. The BSA and SIIA would like to eradicate illegal copying completely, but it is unclear if this is even possible. Possible solutions include making software free or continuing the arms race to protect it. Since it has become such a successful business, open source is probably limited in applicability. Similarly, even with powerful hardware based protections, widespread piracy may decrease, but the problem is not likely to vanish.

B. Software Locks

As discussed above, software piracy has evolved hand and hand with the personal computer revolution. Software piracy was not an issue before 1975 because there were just a few, rich software customers. Everything changed in the new software economy. Now there are millions of poor software consumers that are essentially judgment-proof to legal action. Software locks attempt to solve this problem by preventing software piracy, not punishing it. Just as a physical lock is designed to restrict access, so is a software lock designed to restrict access to a software application. No lock is unbreakable, but the intent is that for most users, it would be cheaper (taking into account time and effort) to purchase a software license than to break the lock.

---

[36] Thomas Locher et al., *Free Riding in BitTorrent is Cheap*, ACM HotNets (2006), *available at* http://www.acm.org/sigs/sigcomm/HotNets-V/locher06free.pdf.
[37] Nazareno Andrade et al., *Influences on cooperation in BitTorrent communities*, Proceeding of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems (2005).
[38] Andrew Kalafut et al., *A study of malware in peer-to-peer networks*, Proceedings of the 6th ACM SIGCOMM on Internet measurement (2006); Seungwon Shin et al., *Malware prevalence in the KaZaA file-sharing network*, Proceedings of the 6th ACM SIGCOMM on Internet measurement (2006).
[39] Kim Komando, *Pirated programs cause problems for users, industry*, USA TODAY (Apr. 19, 2004), *available at* http://www.usatoday.com/tech/columnist/kimkomando/2004-04-19-komando_x.htm.
[40] Adel Ismail Al-Alawi and Mohamed Fathi Abdelgadir, *An Empirical Study of Attitudes and Opinions of Computer Crimes: A Comparative Study between U.K. and the Kingdom of Bahrain*, 2 JOURNAL OF COMPUTER SCIENCE 229-235 (2006).

1. Introduction to Copy Protection and Copy Prevention

Copy protection is the goal of restricting a person's ability to distribute a software application to multiple computers using software locks. The term "protection" is biased in favor of the interests of software industry and their attempts to "protect" their property. The alternative term copy prevention refers to the same thing in a value-neutral manner, but this paper will use the more commonly accepted term "copy protection" for historical reasons.

The controversy regarding copy protection is that it can make a software application less usable for legitimate customers. Without copy protection, a legitimate customer can more easily perform necessary maintenance tasks, such as making backups of the software application for reliability or moving the software application from one machine to another; copy protection often hinders these activities. This trade-off would be more acceptable if copy protection effectively prevented software piracy, but it doesn't. The technology, whose intended effect is to decrease software piracy, has the unfortunate side effect of punishing legitimate customers.

An argument against copy protection is that software can be *cracked*. The original software application can be reverse-engineered and modified in order to create a new version without copy protection. Not only can the cracked version be copied easily, it is also easier to use because it does not contain the locks that aggravate legitimate customers. As a result, legitimate customers may use cracked versions for these reasons. Not everyone possesses the skills to crack a software application, but once it is done, the cracked software can be copied and distributed to anyone.

2. Technologies

a. Nonstandard Magnetic Media Formatting

The late 1970s and early 1980s might be called a golden age of copy protection. Although microcomputers were not then in widespread use, many software applications implemented some form of software lock. These mechanisms were ingenious, each more complicated than the next, making it more difficult to copy the original distribution media.

The year 1978 saw the introduction of many clever software locks for Apple II audiocassettes. The application *Module 6 Blackjack* by Softape suffered from what is now called "code bloat." This program was padded with useless instructions for the sole reason of filling up all 16 kilobytes of system memory. A program from an audiocassette needed to be read in its entirety into memory before it could be copied to another cassette. But this program would overwrite portions of the operating system, thereby making copying impossible. When the next generation of Apple IIs were released with 48 kilobytes of memory, this software lock was easily defeated.[41]

The popular chess program Sargon II by Hayden used a lock known as a two-stage loader. A small loader program was responsible for loading the main program. The main program was stored in an encrypted form that could be decrypted only by the loader. Copying the program from and to another cassette would not work because of a complicated game of "chutes and ladders" with data moved around in memory by the loader until it ended up in the correct location. Other techniques used to implement software locks include storing incorrect checksums, swapping the encoding of 0 and 1, and using different encoding rates rather than the Apple II protocol.[42]

Floppy disk locks were even more sinister. The earliest techniques involved modifying the disk directory that contains the locations of the files. More advanced techniques included hidden tracks (extra tracks towards the end of the disk), half tracks (tracks sitting between two normal tracks), wide tracks (two adjacent tracks with the

[41] Andy McFadden, *Early Copy Protection on the Apple II*, *at* http://www.fadden.com/techmisc/cassette-protect.htm (last visited Dec. 4, 2006).
[42] *Id*.

same data), long tracks (tracks recorded with a slowed motor), synchronization signal counting, nonstandard bit rates, and bit rate changes within a single track.[43] One approach even recorded data in a spiral pattern instead of the standard concentric circles format.[44]

Tools for facilitating software piracy ranged from homegrown hacking tools to commercial products. Omega Microware published an application called Locksmith, whose sole purpose was to copy floppy disks that were supposed to be copy protected. The Apple II magazine, Softalk, ranked Locksmith as the 21st best selling software application of 1981.[45] Other popular disk copying software included Copy II Plus by Central Point Software and Super Disk Copy III by Hartley. Information on how to use these tools was passed around freely on bulletin board systems.

In the end, such software locks fell out of favor as large corporations and even the Department of Defense exerted pressure on the software industry.[46] The technology behind software locks is still studied today within hacker circles attempting to create emulators for the microcomputers of this bygone era.

b. Printed Secrets and Feelies

If the software publishers could not stop people from copying their software, at least they could try to stop them from using it. And to facilitate this, they started including non-software objects with the original software package. The game Deadline by Infocom is regarded as being the first game to include non-software items such as toys and printed materials called *feelies* in an effort to enhance the quality of the game experience.[47] Of this phenomenon Andy Varney writes:

> That golden era of game packaging popularized the non-game items generically called "feelies." You kids today [raps cane on floor] can't imagine the creativity designers and publishers once expended not just on their games, but on their packages and contents. Feelies enhanced the mood and impact of their games, back when graphics were at best simple sprites. Often, feelies also provided a relatively graceful vehicle for authentication-word copy protection.[48]

Many games relied on a low-tech software lock that required a user to enter some information from a printed manual or even a more exotic device such as a code wheel.[49] Some of these printed secrets were obvious locks, such as a table of seemingly random numbers printed on dark red paper to prevent photocopying. Other secrets actually had intrinsic value such as tables of geography statistics from an almanac included with the educational game *Where in the World is Carmen San Diego?* The common requirement for such locks is that it was difficult to copy the secrets. Such locks are no longer practical due to the emergence of the World Wide Web and search engines, and easily publication of secret information.

c. Dongles

One of the most effective software locks is actually a hardware lock called a dongle. For very expensive software, it is economically feasible to distribute a piece of hardware along with the software. The sole purpose of this hardware is for the software to verify its existence. While software and secrets are easy to copy, hardware is not. Dongles have been around since the beginning of the microcomputer age and are still offered by vendors such

[43] Markus Brenner, *Copy Protection vs. Emulators: The battle rages on*, at http://markus.brenner.de/binary/vcf3.pdf (last visited Dec. 4, 2006).
[44] Philip Elmer-Dewitt, *A Victory for Pirates?*, TIME (1986).
[45] *Softalk Presents The Best Sellers*, SOFTALK (1981).
[46] *See* Elmer-Dewitt, *supra* note 44.
[47] Allen Varney, *Feelies*, The Escapist (2006), pp. 12-16.
[48] *Id*.
[49] Eric Lambert, *Old-School PC Copy Protection Schemes*, Vintage Computer and Gaming (2006).

as Aladdin Knowledge Systems and SafeNet.

Dongles vary in their complexity. The earliest dongles may have done nothing more than set a bit high or low on an input port. But just as an arms race existed with media locks, so did dongles undergo an evolution. Robert Best patented a dongle technology that that is now known as a secure crypto processor.[50] This was a separate computer that executed encrypted instructions. Now vital parts of a software application could be encrypted and executed on a special computer that ship only with the application. These types of locks are very advanced and are a key component of the "trusted computing" movement by software publishers.

Dongles are not a complete solution to combating software piracy, having only a narrow scope of applicability. The software must be expensive and specialized enough to justify the additional cost and user dissatisfaction, such as Computer Aided Design (CAD) software. But for software so expensive that only large organizations would use it, legal tools are more effective than software locks. Although hardware costs have decreased over the years, usability problems presently prevent dongles being used for mass-market software applications.

d. License Servers

Not all software piracy is intentional. End User License Agreements (EULAs) differ for every software application, and even a small organization can quickly lose track of whether or not it has purchased enough licenses for all of its users. A license server is designed to help an organization stay honest by acting as a lending library for software licenses. An organization with 30 people might purchase just 10 licenses in order to save money. The license server ensures that no more than 10 different people can use that software application at the same time. Since a license server is designed to keep honest people honest, it is usually not as technically challenging as other types of software locks.

3. Fighting Back

Locks are a passive technology. But software publishers have also developed active technologies to fight software piracy.

MediaSentry created a web crawler that searches the World Wide Web for keywords indicating that a web page might contain software protected by the BSA.[51] The web crawler downloads files and compares them to commercial software applications. If a match is found, the BSA sends a letter to the ISP requesting that the files be removed from their servers.

As previously discussed, much of digital piracy (media or software) now occurs over peer-to-peer networks. A technique called poisoning is general enough to combat all forms of digital piracy, including music, movies, and software. Poisoning decreases the availability of a specific file by injecting a massive number of decoys into the network.[52] This is a highly targeted form of denial-of-service attack. Random decoy injection requires an enormous number of decoys to be injected, which may not be practical. Replicated decoy injection uses a small number of decoys of the same file contents and is much more effective. However, replicated decoy injections can be defeated by using an external reputation system to check for decoys. Replicated transient decoy injection is the same as replicated decoy injection, but changes the file contents periodically in order to defeat an external reputation system. The three types of poisoning can be used simultaneously for increased effect.

---

[50] U.S. Patent No. 4,168,396, (issued Sept. 18, 1979).
[51] L. D. Paulson, *Using web crawlers to fight piracy*, 36 COMPUTER 16-17 (2003).
[52] Nicolas Christin et al., *Content availability, pollution and poisoning in file sharing peer-to-peer networks*, Proceedings of the 6th ACM conference on Electronic commerce (2005).

4. Trusted Computing - The Future?

Trusted computing is a new hardware architecture ostensibly designed to enhance computer security. One of the effects of trusted computing is that it provides a new type of software lock not present on existing computers. It is like having a built in dongle for every software application. A "trusted computer" is trusted by a software publisher not to run software applications without a license. The Electronic Frontier Foundation raises several objections against trusted computing as currently proposed and it is unknown if trusted computing will ever happen.[53] But if it does, digital piracy might then become history.

IV. Legal Responses to Digital Piracy

As explored in the previous sections, computer technology has changed the circumstances and nature of piracy over the years, as the phenomenon moves into the "digital" age. And while content owners have attempted to stem the tide of the unauthorized distribution of software and digital media with technological measures, most U.S. copyright owners employ a strategy that includes the United States legal system as well.

As illustrated by the cases and events discussed below taking us from the 1980s to the present, the advent of digital piracy for the legal system has created a multitude of controversies and conflicts. Much like content owners struggling to adapt technologically to new forms of digital piracy, intellectual property law has had to evolve to address the modern realities of piracy on the Internet. Moreover, the struggle to find a balance between law and technology continues, as with each new legal setback, the technologies that facilitate piracy are modified to avoid future liability.

A. Fighting Digital Piracy with Copyright Law

1. Traditional Copyright Law

a. Digital Media and Software as Copyrightable Subject Matter

The 1976 Copyright Act and later amendments provide the primary statutory basis for modern copyright protection in the United States.[54] Section 102 of the Copyright Act includes protection for such subject matter as "literary works," "musical works," "pictorial, graphic, and sculptural works," "motion pictures and other audiovisual works," and "sound recordings."[55] Software is protected under copyright law as a "literary work."[56]

b. Infringement

Anyone who violates the exclusive rights of a copyright owner (*e.g.*, right of reproduction, right to create derivative works) is liable for copyright infringement.[57] The unauthorized duplication and distribution of copyrighted software or digital media most often constitutes direct infringement of copyright. Infringement liability also extends to parties that facilitate infringement under secondary liability doctrines. Anyone who knowingly "induces, causes or materially contributes" to direct infringement by third parties may be liable for contributory infringement.[58] Anyone who has the "right and ability" to control direct infringement by third parties and has a "direct financial interest" in that infringement may be liable for vicarious infringement.[59]

---

[53] Seth Schoen, *Trusted Computing: Promise and Risk*, Electronic Frontier Foundation (Oct. 1, 2003), *available at* http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php.
[54] *See* 17 U.S.C. § 101 *et seq*.
[55] 17 U.S.C. § 102.
[56] *See* 17 U.S.C. §101; *see also Apple Computer, Inc. v. Franklin Computer Corp*., 714 F.2d 1240 (3rd Cir. 1983). *Computer Associates International, Inc. v. Altai, Inc*., 982 F.2d 693, 712 (2d Cir. 1992) ("Congress has made clear that computer programs are literary works entitled to copyright protection").
[57] *See* 17 U.S.C. § 501(a).
[58] *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc*., 443 F.2d 1159, 1162 (2d Cir. 1971).
[59] *Id*.

c. The Fair Use Defense

Of the various defenses to copyright infringement, the most important to digital piracy law is fair use, allowing people to disregard copyright law in certain situations.[60] Originally a case law doctrine, the fair use defense was codified in 17 U.S.C. § 107 of the 1976 Copyright Act. Section 107 permits the fair use defense in cases such as "criticism, comment, news reporting, teaching ... , scholarship, or research," and leaves a court to evaluate the application of the defense on a case-by-case basis using a variety of factors.[61]

The most well known legal battle over piracy and fair use is the case of *Sony v. Universal*.[62] As discussed previously, Sony developed a popular video tape recording format called Betamax in the 1970s. Wary of the possibility that the public could use Betamax recorders to record and redistribute television shows without authorization, the film industry sued Sony in 1976 for contributory and vicarious copyright infringement.[63] The case was argued all the way up to the Supreme Court, where the court issued a narrow 5-4 opinion in favor of Sony. The Supreme Court noted that although Betamax recorders could be used to pirate television shows, there were "commercially significant noninfringing uses" of the Betamax technology as well.[64] The court explicitly noted that "time-shifting" (recording a television show for later viewing) was a legitimate fair use.[65]

Since 1984, the *Sony* case has often served as the primary protection for technology companies developing new technologies that can potentially be used to "pirate" copyrighted works. And, fair use generally provides the public with some leeway in the unauthorized use of copyrighted works in trivial and/or common sense situations.

2. Software Piracy, Criminal Copyright Infringement, and the NET Act

Before the advent of widespread, high-bandwidth networking, software piracy law mostly dealt with counterfeiters or other for-profit ventures aimed at selling pirated software. Software companies had available civil copyright remedies, and the government used criminal copyright statutes in federal prosecutions. However, the emergence of high-speed networks on college campuses in the early- to mid-1990s for the first time saw widespread *noncommercial* sharing of software.

As mentioned above, throughout 1993 and 1994, David LaMacchia, a 20-year-old MIT student, periodically operated an online bulletin board on MIT's network that enabled people to download unauthorized copies of business and entertainment software.[66] In April 1994, LaMacchia was indicted for conspiracy to commit wire fraud.[67] LaMacchia was not charged under the Section 506 criminal provisions of the Copyright Act, which applied only to commercial situations at the time. In December 1994, the district court granted LaMacchia's motion to dismiss the government's case, noting that the wire fraud statutes did not apply to copyright infringement.[68] Nonetheless, the district court did opine that LaMacchia's actions were at best "heedlessly irresponsible, and at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values," and offered that it was up to the legislature to amend the Copyright Act to include penalties for noncommercial infringement.[69]

In 1997, Congress responded by passing the "No Electronic Theft Act" ("NET") Act, which most notably

---

[60] *See, e.g.*, 17 U.S.C. §§ 107-12.
[61] *See* 17 U.S.C. § 107.
[62] *See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).
[63] *Id.* at 420-21.
[64] *Id.* at 442.
[65] *Id.*
[66] *Student Faces Hardware Charges*, Associated Press, Apr. 7, 1994, *available at* http://onlineethics.org/cases/lamacchia/ap-april7.html.
[67] *Computer Case Raises Questions*, Associated Press, Apr. 10, 1994, *available at* http://onlineethics.org/cases/lamacchia/ap-april10.html.
[68] *United States v. LaMacchia*, 871 F. Supp. 535, 545 (D. Mass. 1994).
[69] *Id.*

amended Section 506 to create criminal liability in some noncommercial situations.[70] Subsequently, many defendants have been found or pled guilty to noncommercial criminal copyright infringement under the NET Act.[71] Notwithstanding this new liability, the Department of Justice still actively pursues criminal copyright infringement cases of for-profit software pirates.[72]

3. Digital Media Piracy and the File Sharing Cases

As noted in Section II of this paper, the explosion of file sharing networks in the late 1990s excited the masses of the media-hungry public and terrified the content industry. By the end of 1999, Napster had formally opened as a company, become the largest file sharing network with millions of users, and been sued by the recording industry. The suit against Napster would become the first in a string of file sharing cases that have shaped, as well as responded to, peer-to-peer network technologies.

a. The *Napster* Case

Napster's peer-to-peer network relied on peer computers connecting to Napster's central indexing server. The server listed media files available on peers and enabled download connections. This central indexing server proved to be Napster's undoing. In *A&M Records v. Napster*, the recording industry alleged that most of the music files traded by the millions of users on Napster were unauthorized copyrighted works.[73] Napster was found liable of contributory and vicarious infringement in district court in 2000, and on appeal to the Ninth Circuit in 2001.[74] The seminal Ninth Circuit case made short work of Napster's various defenses, including a fair use argument that Napster's users were "space-shifting" their music from CDs to computers, much in the same manner that Betamax users "time-shifted" television shows in the *Sony* case. The Ninth Circuit noted that because Napster housed the central index server, it had actual knowledge of the content on its networks, and therefore could not claim *Sony*'s protections.[75] The Ninth Circuit found that Napster's provision of client software and central indexing server constituted a material and knowing contribution to end user infringement, constituting contributory infringement.[76] The Ninth Circuit also found that Napster directly financially benefited from, and had the power to stop, end user infringement, thus meeting the elements for a vicarious liability claim.[77] The Ninth Circuit upheld the district court injunction against Napster, which subsequently shut down and entered into settlement agreements.

b. The *Aimster* Case

After the *Napster* case, the file sharing industry realized that mere knowledge of files traded on a network could give rise to liability, and began adapting peer-to-peer technologies to prevent a company for having direct access to indexing servers. One approach, taken by the file sharing service "Aimster," was to encrypt all communications between peers and the central Aimster index servers. In a court action originally launched by Aimster in 2001, Aimster claimed that it was not liable for secondary copyright infringement because it had no knowledge of the encrypted transmissions going through its network, nor power to block content offered on the

---

[70] *See* No Electronic Theft ("NET") Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997).
[71] *See, e.g.*, Press Release, *Software Pirate Guilty of Copyright Infringement under Net Act*, U.S. Dept. of Justice (May 15, 2001), *available at* http://www.cybercrime.gov/pwa_verdict.htm (trial court verdict finding one defendant guilty of NET Act violations for software piracy, with 13 other defendants pleading guilty); Press Release, *Internet Distributor of Pirated Software Pleads Guilty to Criminal Copyright Infringement*, U.S. Dept. of Justice (Feb. 6, 2004), *available at* http://www.cybercrime.gov/wooSent.htm (sentence after guilty plea to NET Act violation for running a "warez FTP server").
[72] *See, e.g.*, Press Release, *Operator of Massive For-Profit Software Piracy Website Sentenced to Six Years in Prison*, U.S. Dept. of Justice (Aug. 25, 2006), *available at* http://www.cybercrime.gov/ferrerSent.htm (six-year sentence for defendant in software piracy criminal copyright infringement case).
[73] *See A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).
[74] *Id.* at 1010-11.
[75] *Id.* at 1020.
[76] *Id.* at 1022.
[77] *Id.* at 1023.

service. Aimster's argument failed to persuade the district court, which instated a preliminary injunction in 2002 against the service for secondary copyright infringement.[78] On appeal in 2003, the Seventh Circuit upheld the injunction on the basis of Aimster's contributory infringement.[79] The Seventh Circuit found that Aimster employed encryption to deliberately avoid knowledge of the likely copyright infringement occurring on its network.[80]

c. The *Grokster* Case

Other post-Napster file sharing technologies attempted to skirt copyright liability by removing central indexing servers altogether. Some distributed the index server functionality across peers, while others developed peer-to-peer software that worked without any index servers, traversing individual peer nodes exclusively to discover digital content.

Kazaa, Morpheus (distributed by StreamCast Networks) and Grokster were among the next generation of file sharing services to take this approach. All three originally relied on a technology dubbed "FastTrack" that used "supernode" peer computers to provide a network of index servers for other peers. In 2002, the Morpheus system switched to Gnutella, which uses no index servers.[81]

Not surprisingly, the recording industry sued Kazaa, StreamCast and Grokster in 2001 for contributory and vicarious copyright infringement.[82] In addition to pointing out several "non-infringing uses" under *Sony*, the defendants argued that because none of their services maintained a central server, they were not liable for secondary copyright infringement. The defendants asserted that they had no knowledge of the information on third party supernode servers or peers as required for contributory infringement, and could not control the supernodes or peers as required for vicarious infringement. In an interesting turn, the district court (in 2003) and Ninth Circuit (in 2004) both found that the *Grokster* defendants were not liable for secondary copyright infringement.[83]

The victory turned out to be short-lived, as in 2004 the U.S. Supreme Court agreed to hear the recording industry's appeal, which was argued and decided in 2005.[84] While noting that technically, the defendant's respective systems avoided the literal requirements of contributory and vicarious liability, the Supreme Court focused on incriminating internal evidence that the defendants deliberately engineered their system to induce end users to engage in widespread copyright infringement.[85] The Supreme Court set forth a new "inducement" rule, holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[86] Accordingly, the Supreme Court vacated the district and circuit court rulings in favor of the defendants, and remanded the case.[87]

4. Lessons from the Software and Digital Media Piracy Cases

Much of traditional copyright law is built on notions that are no longer accurate or complete, particularly as computer and Internet technologies have evolved from the 1980s, 1990s, and on. As the example of the *LaMacchia* case shows, built-in assumptions of copyright law often fail in the digital age: the traditional criminal copyright and

[78] *See In re Aimster Copyright Litig*., 252 F. Supp. 2d 634 (N.D. Ill. 2002).
[79] *In re Aimster Copyright Litig*., 334 F.3d 643 (7th Cir. 2003).
[80] *See id*. at 650-51.
[81] *See* John Borland, *Morpheus looks to Gnutella for help*, CNET News.com (Feb. 27, 2002), *at* http://news.com.com/2100-1023-846944.html (last visited Nov. 28, 2006).
[82] *See MGM Studios, Inc. v. Grokster, Ltd*., 259 F. Supp. 2d 1029 (C.D. Cal. 2003).
[83] *See id*. at 1046; *see also MGM Studios, Inc. v. Grokster Ltd*., 380 F.3d 1154, 1166-67 (9th Cir. 2004).
[84] *See MGM Studios, Inc. v. Grokster, Ltd*., 125 S. Ct. 2764 (2005).
[85] *Id*. at 2772.
[86] *Id*. at 2780.
[87] *Id*. at 2782.

wire fraud statutes used to prosecute for-profit software pirates simply did not assume noncommercial sharing to be a large problem, until Congress responded with the NET Act.

On the civil side, the development of the file sharing cases from *Napster* to *Grokster* similarly illustrates the difficulties encountered by the legal system in addressing modern forms of digital piracy. While Napster was quickly shut down, the post-Napster file sharing networks assessed the legal conclusions of the *Napster* case to design new technologies that would fare better under copyright law. Although Aimster met a similar fate as Napster, the defendants in the *Grokster* case were successful all the way through the Ninth Circuit. The fact that the Supreme Court had to promulgate an entirely new "inducement" rule to keep the *Grokster* defendants under the yoke of copyright law illustrates that the United States legal system is many respects playing catch up to the technologies underlying modern digital piracy.

B. Protecting "Digital Locks" with the Digital Millennium Copyright Act

While content owners have reliably found relief in court, litigation after the fact has always been an imperfect solution — in most cases, the damage is already is done and a pirated work is in the hands of millions. Thus, as has been explored in previous sections of this paper, content owners also utilize technological content protection mechanisms to prevent any unauthorized use of software or digital media. However, the content protection mechanisms / DRM employed by content owners over the years have mostly met with resounding failure, being easily cracked and permitting the underlying copyrighted content to be extracted and redistributed.

1. The Digital Millennium Copyright Act

In 1998, with much acclaim from the content industry, Congress passed the Digital Millennium Copyright Act ("DMCA") and gave the content industry a powerful legal weapon for fighting piracy: an entirely new category of intellectual property liability for circumventing "digital locks."[88] Section 1201(a) liability extends to any act or tool that breaks a technological protection that prevents unauthorized "access" to digital media or software.[89] Section 1201(b) imposes liability on any tool that breaks DRM protecting software or digital media from unauthorized "copying."[90] Taken together, the anti-circumvention provisions of the DMCA allow content owners to wrap software or media with content protection (against either access or copying), and then sue anyone who breaks the protection — regardless of whether the underlying copyrighted work was actually pirated or not.

2. Stopping the "Lock Pickers" with the DMCA

Soon after the DMCA became effective, content owners quickly began taking defendants into court for breaking technological protection schemes.

a. DVD Encryption and the *DeCSS* Case

As noted in Section II of this paper, most commercial DVD disks protect the underlying video content with a content protection scheme known as Content Scramble System ("CSS"). In late 1999, a Norwegian teenager, Jon Lech Johansen, and two other unidentified individuals developed and publicly released "DeCSS," a popular program that would break the CSS encryption and permit any computer to access or play a CSS-encrypted DVD. In November 1999, Eric Corley, publisher of the hacker magazine *2600*, posted copies and links to the DeCSS program on the *2600* website.

Corley and *2600* were sued shortly thereafter by the major motion picture studios in New York district

[88] *See* 17 U.S.C. §§ 1201-1205.
[89] *See* 17 U.S.C. § 1201(a).
[90] *See* 17 U.S.C. § 1201(b).

court on DMCA anti-circumvention grounds.[91] The defendants argued that the DeCSS program was allowed under reverse-engineering, encryption research, and security testing DMCA Section 1201 exemptions, and the fair use doctrine.[92] The district court dismissed the research and testing defenses quickly, holding that the defendants' bad faith in distributing the program forfeited the defenses.[93]

In their fair use argument, the defendants noted that CSS technologically prevented *any* unauthorized access to the video in a DVD — regardless of whether access / use of the underlying work would have been permissible under traditional copyright law. However, the district court concluded that although fair use is a defense to traditional copyright infringement, Congress had clearly meant to bar the fair use doctrine entirely for DMCA anti-circumvention liability.[94] Accordingly, the district court enjoined the defendants against posting or linking to DeCSS code in 2000.[95] The decision was affirmed on appeal to the Second Circuit in 2001.[96]

b. Digital Music and DMCA Threats

Wary of the ease of unauthorized distribution of digital music, the recording industry set up the Secure Digital Music Initiative ("SDMI") to develop a DRM watermarking scheme for digital music downloads. In September 2000, SDMI initiated a public contest to see if programmers could break the SDMI watermarking technology. A month later, professor Ed Felten and his team at Princeton cracked the entire scheme.[97] Felten was scheduled to present a paper on his team's research at a conference in April 2001, but received a letter from the Recording Industry Association of America ("RIAA") shortly before.[98] In the letter, counsel for the RIAA opined that: "any disclosure of information gained from participating in the [SDMI] Public Challenge … could subject you and your research team to actions under the Digital Millennium Copyright Act ("DMCA")."[99] The RIAA eventually backtracked and pledged not to sue Felten over the disclosure of the technological weakness of the SDMI format, allowing Felten to publish the paper in a later conference.

The recording industry's push to technologically protect compact discs has fared poorly as well. In September 2003, BMG released the first compact disc with copying protection in the United States market, developed by SunnComm Technologies.[100] Alex Halderman, a computer science graduate student at Princeton, posted a paper to his website detailing how to defeat the SunnComm MediaMax copy protection: hold down the "Shift" key when inserting a compact disc into a computer. Halderman was subsequently threatened with a DMCA lawsuit by SunnComm's CEO. A few days later after a strong public backlash, SunnComm reassessed its position and announced it would not sue Halderman.[101]

The SDMI and SunnComm examples demonstrate that not only is the recording industry shifting its legal focus in part to utilize the recent DMCA, but also that the recording industry is truly pushing the bounds of what

---

[91] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).
[92] *Id.* at 319-21.
[93] *Id.* at 320-21.
[94] *See id.* at 322 ("[Congress'] decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.").
[95] *Id.* at 346.
[96] *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).
[97] *See* Ed Felten, *Status of the paper "Reading Between the Lines: Lessons from the SDMI Challenge", at* http://www.cs.princeton.edu/sip/sdmi/ (last updated Aug. 15, 2001).
[98] *See* Electronic Frontier Foundation, *Frequently Asked Questions about Felten & USENIX v. RIAA Legal Case*, *at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/faq_felten.html (last visited Nov. 29, 2006).
[99] Letter from Matthew J. Oppenheim, Senior Vice President, Business and Legal Affairs, RIAA to Edward Felten (Apr. 9, 2001), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010409_riaa_sdmi_letter.html.
[100] John Borland, *Copy-protected CDs take step forward*, CNET NEWS.com (Sept. 12, 2003), *at* http://news.com.com/Copy-protected+CDs+take+step+forward/2100-1027_3-5075656.html (last visited Nov. 29, 2006).
[101] *See* Declan McCullagh, *SunnComm won't sue grad student*, CNET News.com (Oct. 10, 2003), *at* http://news.com.com/SunnComm+wont+sue+grad+student/2100-1027_3-5089448.html (last visited Nov. 15, 2006).

conduct (*e.g.*, research publications, trivial circumventions) will give rise to an actual or threatened DMCA lawsuit.

c. Software Validation and the DMCA

While most of the high-profile DMCA litigation to date has centered on digital media content protection, the DMCA similarly applies to digital locks on software. Parties that distribute tools permitting the circumvention of software validation may face DMCA liability, even where the circumvention is only a small part of an overall distribute program. For example, the developers of bnetd, an open source program that enabled users of Blizzard games to network together to play games outside of Blizzard's own servers, were found liable under the DMCA in district court in 2004 and on appeal in 2005 because their program did not respect Blizzard's built-in software key validation.[102]

3. Lessons from the DMCA Cases

Perhaps the most far-reaching legal impact of the DMCA cases thus far is the rule from the *DeCSS* case that fair use is not a defense to an DMCA anti-circumvention claim, even where the access / use of the underlying copyrighted work is permissible at copyright law. The practical impact is that content owners can now protect software or digital media with technological content protection and sue anyone who breaks the encryption, *regardless* of whether the underlying software / digital media is protected at copyright law. Thus, content owners can enforce far more stringent content protection over digital media and software than they ever could before under traditional copyright law and the *Sony* fair use rules.

More concerning, is the emergence of what some critics call "private copyright" — where access to copyrighted works is governed by dispassionate technology (which permits no exceptions) instead of the law (which has "escape valves" for defenses and fair use).[103] The fear is that now private content owners will dictate what conduct is and is not permissible by wrapping all digital content in technological protection layers instead of Congress promulgating actual copyright law. Backed by the DMCA, content owners can now ensure that their own technological measures control access and use, while the technological measures themselves are protected at law.

V. Conclusion

Computer software, which began half a century ago as essentially an inseparable aspect of unique custom-built systems, has evolved into a global market of commoditized products in its own right. This was a necessary consequence of the proliferation of computer hardware as its size and cost decreased and its performance increased. Personal computing created billions of potential software consumers — and potential software pirates. High-speed networking, the Internet, and peer-to-peer file sharing have provided means for these teeming masses to exchange files without practical limits or restrictions, geographical or otherwise.

Meanwhile, a number of developments have enabled other forms of content, most notably audio and video recordings, to enter the same streams of unauthorized distribution. Popular digital formats beginning with compact disc audio, improving compression schemes, and large inexpensive storage devices have made it possible to store massive collections of music and modest collections of movies in average computers. The cost of storage in particular has fallen so far that an average consumer can easily store more music than an ordinary person could be familiar with. The same may be true for movies before long.

Technical copy-protection schemes for software and other content have been devised, implemented, and

---

[102] *See Davidson & Assocs. v. Internet Gateway*, 334 F. Supp. 2d 1164 (E.D. Mo., 2004); *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

[103] *See* Robin Gross, *Copyright Zealotry in a Digital World: Can Freedom of Speech Survive?*, *in* COPY FIGHTS 190-91 (Adam Theirer & Wayne Crews eds., 2002).

usually defeated; nevertheless efforts continue to reign in the rampant activity unleashed by newly widespread copying and distribution capabilities. In the short term, such mechanisms show little promise for several reasons. Essentially, anything that can be played or executed can in principle be recorded, perhaps with some loss of quality. With digital formats, a single means of access to the raw bits of a digital file enables the production of countless perfect copies. Thus, to prevent such copying, every such means must be eliminated. With such profuse and complicated sources of hardware and software as are available on today's market, this is exceedingly difficult to achieve.

As the technology that enables piracy continues to overwhelm the technology that might prevent it, copyright owners have sought relief in the legal system, primarily under copyright law. From the time software became copyrightable in the 1980s to the explosion of file sharing networks in the 1990s, traditional copyright law has struggled enormously to stop widespread copyright infringement on a scale never previously imagined, and to do this without stifling technological innovation. The introduction of the anti-circumvention provisions of the DMCA at the behest of the content industry has certainly given legal strength to (often failing) technological content protection schemes. However, many critics have expressed concern over the apparently shrinking coverage of fair use for the public, and also over the threats to security research and technology development posed by content industry DMCA posturing. As software and hardware advancements promise to create new and different digital piracy predicaments, a growing issue for the technology industry and public at large is the degree of legal protection that Congress and the courts will extend to the content industry in order to thwart the inherently technological problems of piracy.

The cases of piracy in the media and software industries discussed herein demonstrate that although the widespread unauthorized copying of digital content has been historically infeasible, technological advancements in the last few decades have changed all the rules. The rise of the digital age and perfect copying with essentially zero marginal costs has brought with it the rise of digital piracy. Legal and other mechanisms to prevent unauthorized copying have followed, but despite hardened intellectual property laws and innovations in content protection and rights-management technology, the phenomenon shows no sign of abating. More likely, the factors underlying the accelerating rise in digital piracy will persist, generating more problems for copyright owners and creating new technological, legal, and political controversies in the years to come.