DIGITAL VIDEO COPYRIGHT PROTECTION WITH FILE-BASED CONTENT

By
Patrick Turner

INTRODUCTION

On August 9, 2005 during the Walt Disney Company Earnings Conference Call, Bob Iger, President and CEO-Elect stated what the media industry needed to hear: “We have to truly look more aggressively at (exhibition) window changes ... not only for the studio business but for the TV business. The notion that a product airs on a television network and remains exclusive, in effect, until its rerun airs some six months later, is just one example of what has to change from a windowing perspective,” Iger said. “We can't stand in the way, and we can't allow tradition to stand in the way, of where consumers can go or want to go.”


Between iTunes, Vcast, TiVo PSP, WindowsMedia, cellular phones, public WiFi and available broadband Internet access, the consumer is already well on the way towards multi-platform, on-demand access to worldwide content. After the lessons learned by the recording industry, the question is

*The Author is an attorney with a major media corporation in New York and has practiced electrical engineering for 14 years in areas such as broadcast television systems design, radio frequency transmission and reception, fiber optic data networks, video over telecommunications infrastructures, video compression, computer network administration, and internet working with streaming video. He thanks his wife, Meredith and Professor Michael Botein of New York Law School. B.S., Ceramic Engineering, New York State College of Ceramics, Alfred University (1993); J.D., cum laude, New York Law School (2006); P.E. License, New York, New Jersey; Bar Admissions, New York, New Jersey. The opinions expressed in this article are solely those of the Author.

how the television and motion picture industry will profit from on-demand distribution of media without placing onerous burdens on the consumer.

According to Michael Arrieta, Senior Vice President of Sony Pictures Digital: “The broadcast and media industry is quickly embracing file-based distribution to consumers. Movies and television available as downloadable files is on a fast track towards acceptance and indeed is becoming commonplace. The question of adequate copyright protection of the intellectual property is paramount to the studios.”

Who tracks content and how? Is it acceptable to track the content use as a necessary component of copyright protection? How far do viewer’s rights extend? Does fair use survive in a digital file based world? One thing is clear, legally enforceable copy protection is a necessary burden.

According to U.S. copyright law, Section 501,

(a) Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122 or of the author as provided in section 106A (a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be . . .

Digital cable, cable on demand, and direct-to-home satellite already use Digital Rights Management (DRM) technology to prevent digital or analog copies of protected content. Online, Google, Apple, RealNetworks, and Microsoft also use DRM, so it appears that video copyright holders are pre-empting the problem that the music industry failed to adequately confront.

A. United States Copyright Law

The U.S. Constitution provides for patent and copyright protection in Article 1, Clause 8, Section 8. In establishing the role of the Congress, the Constitution provides that: “The Congress shall have power … To promote the progress of science and useful arts, by securing for limited times to authors

---

3 Note: Walmart’s online store allows customers to purchase full length television programs and movies. See http://mediadownloads.walmart.com/mmce/jsp/storeHome.jsp.
and inventors the exclusive right to their respective writings and discoveries.”

The first U.S. Congress passed the Copyright Act of 1790 to protect copyright holders of maps, charts and books for a term of fourteen years, renewable for another fourteen years. Congress modeled the Act after the British Statute of Anne published in 1710. In 1831 the Copyright Act was amended to extend the term of protection to twenty-eight years, with a possible fourteen-year extension in order to match protections in Europe. In 1909, Congress expanded the scope of coverage of copyright protection to include all original works of authorship and extended the possible renewal term to twenty-eight years.

In 1976, Congress passed a major revision to copyright law as a result of technological developments and the expected ascension to the Berne Convention for the Protection of Literary and Artistic Works. The revision extended copyright protection to the author’s life, plus fifty years and codified the judicially created exception to copyright law called “fair use” where certain otherwise infringing activities are granted legal protection.

The doctrine of fair use for activities such as parody, comment, news reporting, teaching, scholarship, and research is described in the Copyright Act with a four-factor test:

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work;
3. Amount and substantiality of the portion used in relation to the

---

8 See SAMUELS, supra note 6, at 3.
9 Id.
11 See Campbell v. Acuff-Rose, 510 U.S. 569 (1994) (holding 2 Live Crew’s rap version of Roy Orbison’s “Oh Pretty Woman” was fair use as a parody despite the commercial nature of the recording).
copyrighted work as a whole; and
4. The effect of the use upon the potential market for or value of the copyrighted work.

In 1994, the United States signed the Uruguay Round Agreements Act (URAA) implementing the General Agreement on Tariffs and Trade (GATT) that established the World Trade Organization and included the Trade Related Aspects of Intellectual Property (TRIPS) agreement, which added provisions to U.S. copyright law in accordance with the World Trade Organization (WTO). The URAA modified the original GATT treaty from 1947. Most of the provisions of the WTO Agreement took effect on January 1, 1996.

In 1998 Congress passed the Sonny Bono Copyright Term Extension Act (CTEA), unkindly known as "The Mickey Mouse Protection Act," extending copyright protection to the life of the author plus seventy years (ninety-five years for works of corporate authorship). Mickey Mouse, who began his career on the cartoon short “Steamboat Willie” in 1928, would have lost copyright protection in 2003. The Act gave Disney Corporation, along with all legacy copyright holders, a reprieve so that Mickey is protected until 2023. In Eldred v. Ashcroft, the Supreme Court upheld the CTEA as a valid exercise of congressional powers.

---

15 The GATT treaty was signed by President Clinton on December 8, 1994 with the agreement effective on January 1, 1995 with one year provided for implementation of most provisions providing for full enforcement as of January 1, 1996. For countries and dates of ascension see http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited Mar. 5, 2007). For U.S. Copyright Office information on the implications of the URAA to U.S. copyright law see http://www.copyright.gov/title17/92appiii.html (last visited Mar. 5, 2007).
B. WIPO and The Digital Millennium Copyright Act (1998)


Regarding the TRIPS agreement, according to the WTO:

… With respect to copyright, parties are required to comply with the substantive provisions of the Berne Convention for the protection of literary and artistic works, in its latest version (Paris 1971), though they will not be obliged to protect moral rights as stipulated in Article 6bis of that Convention.

The birth of legally enforceable DRM for digital video began with the signing of the WIPO Copyright Treaty. Article 11 of the WIPO Treaty contains the following language:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted

---

20 See Berne Convention, supra note 10.
Reinforcement of U.S. legal protection for copyrighted material came in 1998 with passage of the Digital Millennium Copyright Act (DMCA). The DMCA incorporated agreements from the WIPO Copyright Treaty. The DMCA has five titles:

- Title I: WIPO Copyright and Performances and Phonograms Treaties Implementation Act
- Title II: Online Copyright Infringement Liability Limitation Act
- Title III: Computer Maintenance Competition Assurance Act
- Title IV: Miscellaneous Provisions
- Title V: Vessel Hull Design Protection Act

Section 102 of the DMCA incorporates the language of Article 11 of the WIPO Copyright Treaty and adds a new Section 12 to Title 17 of the U.S. Code. In accordance with the WIPO treaty, section 1201(a)(1)(A) of the Act states, “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

Section 1201(a)(2)(A) of the DMCA adds teeth to the law, and provides the most controversial text in the act: “No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that … is primarily designed or produced for the purpose of circumventing a technological measure that controls access to a [copyrighted] work.”

The DMCA added criminal penalties for circumventing anti-piracy measures in commercial software, outlawed manufacturing technology to crack copy protection (except for research), and provided conditional exemption from liability for Internet service providers for copyright infringement conducted on networks. The DMCA provisions on circumventing anti-piracy provisions have serious implications for personal

---

25 Id.
27 RIAA v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003) (holding that Verizon was not required to identify users of its Internet service who were infringing on copyrights under 17 U.S.C. § 512 (2006)).
fair use of purchased content.

In 1976, Universal City Studios, Inc. and Walt Disney Productions sued Sony Corporation of America in District Court of the Central District of California for vicarious copyright infringement as a result of manufacturing and selling the Betamax videocassette recorder.\textsuperscript{28} The District Court held that non-commercial home use of material broadcast over the air was fair use and was not copyright infringement and that Sony had no direct knowledge of infringing activities.\textsuperscript{29} The California Court of Appeals for the Ninth Circuit reversed the copyright claim.\textsuperscript{30} The Ninth Circuit held that the infringing use was not a “productive use” and that Sony had knowledge of the infringement because the recording of copyrighted material was the “most conspicuous use” of the device.\textsuperscript{31}

The Supreme Court held in a 5-4 opinion in \textit{Sony Corp v. Universal City Studios}, that private non-commercial time shifting by home viewers for delayed playback is a fair use of copyrighted material that is not copyright infringement.\textsuperscript{32} The Supreme Court noted that the District Court had evidence that time shifting actually increased television access to viewers, which indicated a benefit of VCR use to plaintiffs, the motion picture studios.\textsuperscript{33} In the dissent, Justice Blackmun stated that “time-shifting” and “library building” are copyright infringement and the doctrine of fair use has no application to “purely personal consumption on the scale involved in this case.”\textsuperscript{34} In a notable foreshadowing of the “Broadcast Flag,” infra, Justice Blackmun suggested that perhaps Sony may “build a VTR [video tape recorder] that enables broadcasters to scramble the signal of individual programs and ‘jam’ the unauthorized recording of them.”\textsuperscript{35}

\textit{Sony Corp. v. Universal City Studios} gave consumers the right to time-shift (create personal copies of) television and movies. It is arguable that time shifting as fair use is a legal fiction, and thus consumers never really had control over the content to begin with. However, consumers have become used to the notion of flexible use of purchased content and restrictions over

\begin{itemize}
\item \textsuperscript{28} Universal City Studios, Inc. v. Sony Corp. of Am., 480 F. Supp. 429 (D. Cal. 1979).
\item \textsuperscript{29} \textit{Id}.
\item \textsuperscript{30} Universal City Studios, Inc. v. Sony Corp., 659 F.2d 963 (9th Cir. 1981).
\item \textsuperscript{31} \textit{Universal City Studios, Inc.}, 480 F. Supp. 963.
\item \textsuperscript{32} \textit{Sony Corp. v. Universal City Studios}, 464 U.S. 417 (1984).
\item \textsuperscript{33} \textit{Sony Corp.}, 464 U.S. at 425.
\item \textsuperscript{34} \textit{Id} at 495.
\item \textsuperscript{35} \textit{Id} at 494.
\end{itemize}
personal use are an imposition.

The DMCA does provide some weak wording in Section 1201(a)(1)(B)-(D) that allows the Librarian of Congress to conduct a periodic review on the effects of circumvention of technological measures on the market for or value of copyrighted content. Consumers should probably not expect the Librarian of Congress to diligently investigate why digital content protection is interfering with playback of the latest “Spider Man” sequel.

C. Fair Use and Flexibility vs. Content Control

Current technology, available to consumers, allows for perfect digital reproduction of digital content, which seriously complicates the issue. Despite a recent Supreme Court challenge in MGM Studios v. Grokster, Sony remains good law. It is very possible that if the Sony Betamax videocassette recorder had created a perfect digital copy of television programs or movies, the 5-4 decision would have come out differently.

If we look to the past to predict the future of digital video copyright issues, the most relevant history comes from looking at online music sales, the DVD industry, and the Digital Millennium Copyright Act. Music sales are relevant because the delivery and portability are nearly identical with programs and movies. Further, the Apple iTunes music service is now selling video and movies. Services such as Cinemanow and soon Netflix and Sony are touting movies for download.

I MUSIC INDUSTRY FILE SHARING

Audio files are easily distributable due to the relatively small size and low bit rate. An uncompressed stereo audio song at compact disc (CD) quality sampled at 44.1kHz (44100 samples per second) with 16-bits per sample has a bit rate of ~1.5Mbit per second, resulting in a file size of ~10MBytes per minute. A full-length uncompressed 2-minute song is 20 Mbytes of storage, easily fitting on a memory stick or compact disc. An MPEG 1, Layer 3 (MP3) file at 128 kbit/s takes about 10 percent (~2 Mbytes) of the space of

uncompressed audio with a minor quality impact.\textsuperscript{39} The difference is degraded high frequency response above 16 kHz, however with most music an average listener will generally not notice a difference.\textsuperscript{40} A complete album with twenty songs can be downloaded in less than ten minutes on a broadband Internet connection.

MP3 audio files are easily copied with identical quality over subsequent generations. MP3 files can be created from purchased compact discs using commercially available software, including the Windows Media Player\textsuperscript{41} or the free download of the RealPlayer.\textsuperscript{42} Because of the small size and high quality, MP3 files are ripe for theft. The music industry has been forced to deal with digital file based copyright infringement on a large scale.

A. Piracy

In late 1999, Napster established a cottage industry in peer-to-peer file sharing, enabling a peak of twenty-six million worldwide users to exchange music free of charge by February 2001.\textsuperscript{43}

In January 2000, after millions of MP3 files had been exchanged on the public Internet, A&M Records along with all the major recording labels in the United States sued Napster for “contributory and vicarious copyright infringement” under U.S. Copyright Law (17 U.S.C.) citing the provisions of the Digital Millennium Copyright Act.\textsuperscript{44} Dr. Dre and Metallica also filed

\textsuperscript{40} See MP3’s Tech - An Examination of the Correlation Between Perceived Sound Quality and Frequency Response, http://www.mp3tech.org/tests/pm/MP3-160k.htm (last visited Mar. 5, 2007).
lawsuits after new songs were discovered on Napster prior to official release.\textsuperscript{45} Napster called itself “the world’s largest MP3 music library.”\textsuperscript{46}

In the District Court for the Northern District of California, the recording labels sought and won a preliminary injunction enjoining Napster from copyright infringement without permission from rights holders. The court held the plaintiffs had a reasonable likelihood of success for contributory copyright infringement by showing direct infringement by users and vicarious copyright infringement by showing that Napster had the “right and ability to supervise the infringing activity and also has a direct financial interest in such activities.”\textsuperscript{47} The court rejected defenses based on fair use and substantial non-infringing uses. Napster also tried to invoke the 17 U.S.C. §512(d) DMCA safe harbor provisions protecting a service provider from liability; however the court stated that “section 512(a) does not cover Napster because, unlike protected Internet service providers, Napster does not act as a mere conduit for file sharing.”\textsuperscript{48} The Court of Appeals for the Ninth Circuit upheld the preliminary injunction forcing a shutdown until Napster could adequately prevent copyrighted works from being shared with its service.\textsuperscript{49}

After the Ninth Circuit, the case was settled for a $26 million dollar payment to compensate artists for copyright infringement and as against future lost royalties. Ultimately Napster declared bankruptcy, and was acquired by Roxio and used to re-brand the “Pressplay” legal online music sales Web site.\textsuperscript{50} The key to Napster was that the service provided a central database and data storage used for copyright infringement.

Unfortunately for the RIAA, the publicity inspired others to find ways around the Napster precedent. Aimster and Grokster both tested the limits of the DMCA.\textsuperscript{51} Aimster was originally developed to allow users of AOL Instant Messenger to share files, adding the ‘ster from Napster. Aimster was renamed

\textsuperscript{49} A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).
\textsuperscript{50} Roxio Acquires Pressplay For $40 Million, N.Y. TIMES, May 20, 2003, at C6.
Madster after an AOL trademark infringement suit.\(^{52}\)

A group of music industry copyright holders sued Aimster (Madster) for “contributory copyright infringement.” The District Court in the Northern District of Illinois entered a preliminary injunction shutting down Aimster based on a likelihood of success on the merits by the copyright holders.\(^{53}\) On appeal, the Court of Appeals for the Seventh Circuit held that although the Aimster service was capable of non-infringing uses, there was no evidence it had ever been used for non-infringing use.\(^{54}\) The court noted that Aimster provided “…computerized tutorials instructing users of the software on how to use it for swapping computer files” which were an invitation to infringement.\(^{55}\)

Aimster was not truly peer-to-peer, as there was centralized management of the servers. Aimster (Madster) was ordered to shut down its servers after failing to comply with the injunction. The founder, John Deep, declared bankruptcy after a failed appeal to the Supreme Court, and the Madster Web site is currently soliciting claims against Mr. Deep.\(^{56}\)

The most direct challenge to \textit{Sony v. Universal Studios} arose with a service called Grokster. Similar to Napster, Grokster created freely available peer-to-peer file sharing software. The difference in Grokster software was that no central database existed for tracking content,\(^{57}\) rather Grokster made money through advertising revenue from streaming ads to users. MGM Studios along with twenty seven other copyright holders sued Grokster and Streamcast Networks (Morpheus) for contributory copyright infringement.\(^{58}\) Sharman Networks Kazaa was originally a defendant, but was dropped because it was based in Vanuatu.\(^{59}\)

\textit{Grokster} argued, citing \textit{Sony v. Universal}, that like the Sony Betamax videocassette recorder, Grokster software was capable of “substantial non-infringing uses [which] could not give rise to contributory liability for

\(^{53}\) \textit{In re} Aimster Copyright Litigation, 252 F.Supp.2d 634 (N.D. Ill. 2002).
\(^{54}\) \textit{In re} Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).
\(^{55}\) \textit{Id.} at 646.
infringement unless the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge.” 60 The District Court in the Central District of California 61 and Ninth Circuit Court of Appeals found these arguments persuasive and held for Grokster. 62

In a highly visible case, the U.S. Supreme Court unanimously reversed the Ninth Circuit Court of Appeals, holding Grokster (and Morpheus) liable for contributory copyright infringement. The Grokster case was widely considered the first direct challenge to Sony v. Universal since 1984. The Court held that each company was knowingly satisfying a demand for copyright infringement comprised of former Napster users, that neither company had any filtering tools to diminish the infringing uses of its software, and that both companies profited by high volume users of the service which overwhelmingly involved copyrighted material. Justice Souter stated “[t]he unlawful objective is unmistakable.” 63 The Court found no lack of evidence of actual infringement by recipients of the Grokster software.

The Court did not review Sony v. Universal any more than necessary to describe the issues in the case. In 2005, Grokster ceased operation. 64 The Court left alone the fair use exception carved out in Sony. The question is when exactly does duplication or reproduction become copyright infringement? According to recent case law in Kelly v. Arriba Soft Corp, “[t]o establish a claim of copyright infringement by reproduction, the plaintiff must show ownership of the copyright and copying by the defendant.” 65 Despite the success of the recording industry with peer-to-peer file sharing, much damage has already been done. The RIAA has become the designated enforcer of music industry copyright protection.

The RIAA has filed thousands of subpoenas and lawsuits against people for copyright infringement, including notable cases against children. In 2003, the RIAA sued 12-year-old Brianna LaHara of New York, who lives in public housing and was a paying subscriber of the Kazaa subscription service,

60 Grokster, 545 U.S. at 914.
63 Grokster, 545 U.S. at 940.
seeking $150,000 per song downloaded. In a settlement with the RIAA, Brianna’s family agreed to pay $2,000 to dismiss the claims and quiet the bad publicity for the music industry.

According to studies by the Pew Internet and American Life Project in 2004, the RIAA lawsuits cut down peer-to-peer file sharing by 50 percent. Although the RIAA lawsuits have been wildly unpopular, it appears that the RIAA has succeeded in part in making the public aware that file sharing is illegal copyright infringement. The economic success of the RIAA lawsuits to drive users towards legal (paid) content purchase is unclear. However, recent success with iTunes and 99-cent songs tends to indicate the RIAA has partly been successful.

The Internet2 distribution system, mainly used today between universities, provides vastly improved data delivery at up to 100 Mbit/s to the desktop. Although the system is still experimental at this time, it has not stopped peer-to-peer file sharing. In April 2005, the RIAA and MPAA filed lawsuits against 405 college students using the Internet2 backbone for copyright infringement using the peer-to-peer service i2hub. Students from Boston University, Carnegie Mellon University, Columbia University, Georgia Institute of Technology, Harvard University, Massachusetts Institute of Technology, Ohio State University, Princeton University, and University of Southern California were involved. Using the Internet2 a full-length movie can be copied in about five minutes.

In an effort to thwart CD copyright infringement, in 2005 Sony BMG included software developed by First4Internet (XCP) and SunnComm

---

72 *Id.*
MediaMax on over 24 million music CDs that installed a user undetectable “Rootkit” in the system registry of consumer PCs. A rootkit is hidden computer code that can execute instructions undetected. A rootkit is generally invisible to the user and is frequently used as an exploit by malicious software programmers to hijack processes on PCs. The danger is that rootkits are very hard to find and eliminate, which means that a PC may be infected for years unbeknownst to the owner. The Sony rootkit was shipped with software that included a “clickwrap” End User License Agreement (EULA) on behalf of First4Internet and MediaMax. The rootkit was discovered by Mark Russinovich, a well-known developer of free Microsoft Windows utilities and the process for discovery was posted online and quickly picked up by other news services.

The resulting uproar by consumers led to lawsuits by the Texas Attorney General, the Electronic Frontier Foundation and a class action lawsuit in California. In December 2005, Sony agreed to settle the class action lawsuits including removal of all affected CDs from the market and allow users to exchange XCP CDs for non-protected CDs. The Sony CD rootkit debacle could just as easily have been discovered on a DVD, and over time will likely be repeated with HD-DVDs and Blu-Ray discs.

“Fingerprinting” is a new mechanism that has emerged as a possible technology for music (and video) content enforcement with file sharing web sites and sites hosting user generated content. Fingerprinting involves using a sample of music or video clip to create a digital fingerprint of the unique

---

79 Vendors such as Audible Magic and GraceNote supply this service to online providers. Philips MediaHedge is a proposed video fingerprinting technology.
combination of digital sound values or video picture elements. This fingerprint may be compared electronically at high speed against a company’s entire library of stored clips, such as those on YouTube, to determine if any of the stored content matches the fingerprint. If fingerprinted content is discovered the copyright owner may demand it be taken down. MySpace has already acknowledged using GraceNote for audio. The downside to using fingerprinting is that all content in a library must be processed to develop a fingerprint database and it is unclear how fingerprints survive degradation from down sampling to lower bit rates.

B. Implications for the Television and Film Industry

The music industry has been forced to deal with digital file based copyright infringement on a large scale. The television and motion picture industry has the benefit of larger files that require higher data rates, which result in greater difficulty of illegal sharing. However, the DVD format, discussed in the next section, has been a great test case for digital content protection, as both a fabulous sales success and a powerful tool for copyright infringement. New technologies like HD-DVD, Blu-Ray, BitTorrent and the SlingBox will continue to bring the digital content protection issue squarely to the forefront of modern media.

II DVD CONTENT PROTECTION

A. The DVD Format

Since the release of the DVD format in 1997, there have been over 100 million DVD players sold in the United States alone, according to the Consumer Electronics Association (CEA). The DVD-Video standard was created by a consortium including Philips, JVC, Matsushita, Mitsubishi, Hitachi, Pioneer, Sony, Thomson, Time Warner, and Toshiba. The format

83 The “DVD Forum” includes the founding format creators and is responsible for guiding the format in consumer electronics. New vendors of DVD based products may purchase one of several confidential “books” from the forum
uses a 12-cm disc (or smaller 8 cm disc), identical in size to an audio Compact Disc and supports one main stream of video, generally MPEG-2 with up to nine possible camera angles, up to eight audio streams including Dolby Digital, MPEG-1, MPEG-2, PCM, or DTS, and navigation menus, still images, interactivity, and random access.\footnote{180}

The standard dual-layer DVD used for movies can hold 9.4 Gigabytes (1 Gigabyte = 1,073,741,824 bytes of data), allowing for capacity of a full-length movie using variable bit rate MPEG-2 compression between 3 and 10 Mbit/s at 720 horizontal pixels x 480 vertical lines of resolution for NTSC displays (720 pixels x 576 lines for PAL), including multiple tracks of CD quality audio.\footnote{84} The DVD player has been the most successful consumer electronics product in history.\footnote{86}

Along with the success of the DVD format has come piracy and legal challenges to copyright protection technology. The MPAA claims the DVD piracy problem has reached epic proportions because “[a]ccording to the most recent estimates available from the International Federation of Phonographic Industries (IFPI), the movie industry lost more than $4.5 billion worldwide to physical piracy in 2003.”\footnote{87}

To prevent illegal copyright infringement, DVDs may include one of many copy protection mechanisms including:

- Content Protection for Prerecorded Media, Content Protection for Recordable Media (CPPM), (CPRM)
- Digital Transmission Content Protection (DTCP)
- Copy Generation Management System - Analog (CGMS-A)
- Macrovision Analog Protection System (APS) – Copyguard
- Content Scrambling System (CSS)


Id. \footnote{86}


• Watermarking (Verance)
• Region Codes (Mandatory for DVD Players)
• Disabled User Operations (prevents some types of playback operations)

The difficulty is that none of the copy protection mechanisms are mandatory for manufacturers of DVD players with the exception of region codes. As with all copy protection mechanisms for DVDs, the standard depends on cooperation by the copyright holders and the manufacturers.

1. **CPRM/CPPM, The 4C Entity LLC**

IBM, Intel, Matsushita and Toshiba created a limited liability corporation dubbed the “4C Entity” (four companies) and jointly created the Content Protection for Recordable Media and Pre-Recorded Media (CPRM) / (CPPM) specifications. The 4C Entity created the Copy Protection System Architecture (CPSA) as a framework for overall copy protection and watermarking in cooperation with Secure Digital Music Initiative and the Copy Protection Technical Working Group.\(^{88}\) The CPPM/CPRM includes copy protection for pre-recorded, recordable DVD media and Flash memory. IBM, Intel, Matsushita and Toshiba all manufacture components of DVD players and thus can add CPPM/CPRM technology to products.\(^{89}\)

2. **The DTLA Consortium, DTCP-5C**

The Five Company (5C) Digital Transmission Content Protection (DTCP) specification was created by Hitachi, Intel, Matsushita, Sony and Toshiba as members of the Digital Transmission Licensing Administrator (DTLA) working in the Copy Protection Technical Working Group (CPTWG). The standard defines a cryptographic protocol for protecting audio/video entertainment content from illegal copying as it moves across high speed digital buses such as Universal Serial Bus 2.0 (USB 2.0) or Institute of Electrical and Electronic Engineers standard 1394 (IEEE 1394 also

\(^{88}\) 4C ENTITY, CONTENT PROTECTION SYSTEM ARCHITECTURE: A COMPREHENSIVE FRAMEWORK FOR CONTENT PROTECTION 6 (2000), http://www.4centity.com/data/tech/cpsa/cpsa081.pdf. Note: The CPSA framework describes an overall proposed structure for content protection, but only parts are implemented on consumer electronics.

\(^{89}\) 4C ENTITY, POLICY STATEMENT ON USE OF CONTENT PROTECTION FOR RECORDABLE MEDIA, (CPRM) IN CERTAIN APPLICATIONS, http://www.4centity.com/data/tech/cprmfactsheet.pdf.
referred to as Firewire). Most personal computers include Firewire, USB or both.

If a consumer attempts to copy a file from a DVD using Firewire, DTCP copy protection may prevent it. “Only legitimate entertainment content delivered to a source device via another approved copy protection system (such as the DVD Content Scrambling System) will be protected by this copy protection system.” If content is ‘cracked’ or decrypted, it will pass through DTCP protected data bases without problems.

3. *Macrovision Copy Protection*

DTCP protects on the digital communication bus, contrasted with Macrovision, which protects at the analog receiver device. According to the Macrovision Web site: “Macrovision Corporation develops digital rights management and software licensing technologies to combat widespread casual digital piracy while offering solutions that enable our customers to electronically control the use of digital content and software, and to build significant new revenue models.”

Macrovision sells software called ACP-VOD that adds content protection for media received via direct broadcast satellite or cable video on demand (VOD). The “ACPe” software prevents copying on DVD recorders and distorts copies made on VHS recorders, and prevents permanent copies on hard drives or digital video recorders (DVRs).

Macrovision is used on over 75 percent of DVDs sold in the United States and virtually all consumer VCRs.

---

4. Copy Generation Management System Analog

In DVD-Video streams, CGMS-A embeds Copy Control Information (CCI) into the Extended Data Services (XDS) of line 21 of the NTSC video signal (which also contains closed-captioning data).\(^{95}\) CGMS-A is a standard published by the International Electrotechnical Commission as IEC 61880.\(^{96}\)

The value of the CGMS CCI tells compliant downstream recording devices whether they can copy the signal without constraint (CCI bits set to 00), record one generation of copies (01), or make no copies at all (11).\(^{97}\) HBO uses CGMS-A for restriction of multiple copies of analog content.\(^{98}\) A CGMS-D system was pursued, however it appears to be subsumed into other forms of protection.\(^{99}\)

5. Content Scrambling System

CSS was agreed upon in 1996 as the first protection mechanism for copy protection of DVDs.\(^{100}\) CSS is the official DVD rights management system that was incorporated in the DVD standard upon release. The rationale was that movie studios would be hesitant to release movies on DVD if there were no native DRM. CSS involves a 40-bit key encryption system that may only be decrypted by licensed CSS keys. The DVD Copy Control Association “DVD-CCA” administers CSS licenses.\(^{101}\) CSS has been the subject of substantial litigation, discussed later.

---


\(^{97}\) Labriola, *supra* note 95 at Part I.


\(^{99}\) Labriola, *supra* note 95 at Part II.


6. **Verance Watermarking**

Verance is a private company that sells both DVD-audio and video watermarking technology. Verance will likely become a bigger player with respect to HD-DVD and Blu-Ray discs. Watermarking technology is used for content tracking, and could be used for protection if the video circuitry was capable of detecting the watermark.

7. **Region Codes in DVDs**

All DVD players have a hardware region code embedded by the manufacturer based upon where they plan to sell the player, to control distribution of content. This is one primitive way to reduce copyright infringement.

All legally manufactured DVD players have region codes, but not all discs have region codes. DVD players only play discs that possess the correct region code, or discs with no code. Region codes do not apply to recordable DVDs (DVD-R/W, DVD+R/W) or DVD-Audio. The PlayStation2 (PS2) and Xbox have different region codes for games. Third party tools are able to extract the PS2 region code.

Copyright holders working with manufacturers of CDs have the option to embed a region code into a disc. Most Hollywood releases have region codes embedded that restrict playback. Region codes cannot be changed and never time out.

As with all copy protection technology, savvy hackers have illegally created region code disabled DVD players that play all DVDs from all regions. This is more visible in Europe, Australia and Asia. The trouble with hacking region codes is that often the source format is an incompatible

---

104 Id.
105 Id.
NTSC or PAL derivative that will not play back on the viewer’s television. For example, if the manufacturer creates a disc for the NTSC format with 525 lines at 59.95 Hz with a 3.58 MHz color subcarrier, it will generally not play on a PAL device expecting 625 lines at 50 Hz with a 4.43 MHz color subcarrier. The United States, Canada and Mexico use the NTSC standard, whereas Europe generally uses PAL (or SECAM in France and Eastern Europe). Even if the DVD player can decode multiple formats, often television sets are limited to a single standard. Regions are generally broken up by continent.

In March 2001, the space shuttle Atlantis docked at the International Space Station with two Sony DVD players. The question is, what region code applies to space? Apparently, the astronauts received a possibly illegal multi-region player to accommodate the international residents. The threat of copyright infringement in space appears to be minimal.

B. DVD Copy Protection – DeCSS

CSS copy protection uses relatively weak 40-bit key encryption. In 1999, a 15-year-old Norwegian teenager, Jon Lech Johansen, cracked the CSS encryption. CSS was not patented; rather it was a trade secret. Johansen created DeCSS to Decrypt CSS so he could watch DVDs on his Linux based computer, which, at the time, did not support a CSS player. Johansen was prosecuted for violation of copyright and invitation to wide-scale piracy by Økokrim, a Norwegian crime unit, following complaints by the U.S. based DVD Copy Control Association (DVD-CCA) and the Motion Picture Association of America (MPAA). In 2004, an Oslo court acquitted Johansen of all charges. The Norwegian court held there was no evidence that Johansen had used DeCSS for illegal purposes, nor was it illegal to watch DVDs purchased legally.

At the same time Johansen was in court, American Andrew Bunner posted the DeCSS source code on a Web site hosted by servers located in California. The DVD-CCA was granted an injunction in Superior Court of Santa Clara County to force Bunner to remove the source code from his Web site. The DVD-CCA relied on the Uniform Trade Secrets Act (UTSA), adopted by California under California Civil Code §3426.1. The Superior Court held that CSS and master keys were trade secrets; that publication of trade secrets on the Internet did not destroy trade secret status; that the publication of DeCSS discloses those trade secrets; and the creator of DeCSS acquired the trade secrets by improper means. Although reverse engineering of a trade secret is generally legal, a very specific click-wrap license in the CSS standard precluded reverse engineering.

The Court of Appeals for the Sixth District reversed, citing an invalid prior restraint. The California Supreme Court reversed the Court of Appeals for the Sixth District, finding no valid First Amendment protection and a knowing violation of the UTSA and reinstated the injunction.

The California Supreme Court, finding no legitimate public interest at stake to justify First Amendment protection, upheld the injunction and remanded to the Court of Appeals to determine if the Superior Court properly issued the preliminary injunction. On remand, the Court of Appeals reversed the trial court because DeCSS had been so widely distributed as to lose its trade secret status.

Carnegie Mellon University generously provides a Web site directory of the most popular CSS descramblers and links to source code. There has

---

114 Id. at 346.
116 DVD Copy Control Assn., 113 Cal. Rptr. 2d at 350.
118 Id. at 889.
been an unofficial competition among programmers to produce the smallest possible CSS descrambler, with the current size less than 500 bytes (less than 10 lines of code). Before Bunner was finally decided in 2004, publication of DeCSS could have involved criminal penalties under the DMCA.

At the same time that Andrew Bunner was litigating on First Amendment grounds, Universal City Studios and seven other motion picture studios sued Eric Corley of 2600 Enterprises in United States District Court for the Southern District of New York, after he described DeCSS and posted the DeCSS source code on the 2600: The Hacker Quarterly web site.\textsuperscript{121}

The District Court imposed a preliminary injunction to prevent 2600 Enterprises from posting the DeCSS source code under the “anti-trafficking provisions” in Digital Millennium Copyright Act.\textsuperscript{122} 2600 Enterprises was further restricted from linking to the code on other Web sites.\textsuperscript{123}

Corley and 2600 Enterprises appealed the injunction and argued the same First Amendment case as Bunner; however the Court of Appeals for the Second Circuit affirmed the District Court’s injunction as a legitimate restriction on speech.\textsuperscript{124} The court noted that the computer software was content-neutral and thus the “regulation [DMCA] must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest.”\textsuperscript{125} The court stated that the government had a substantial interest in preventing copyright infringement, and that restricting the posting of DeCSS plainly serves that purpose.\textsuperscript{126}

DeCSS even showed up on store shelves afterward. St. Charles, Missouri based 321 Studios began selling software that relied on DeCSS called DVD-X Copy and DVD Copy Plus to allow consumers to make “backup copies” of commercial DVDs. As pressure mounted by the motion


\textsuperscript{121} 2600.com http://www.2600.com/ (last visited Mar. 25, 2007).


\textsuperscript{123} \textit{Id.}

\textsuperscript{124} Universal City Studios Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

\textsuperscript{125} \textit{Id.} at 454 (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622 (1994)).

\textsuperscript{126} \textit{Id.} at 456.

187
picture industry, 321 Studios filed suit in 2002 in the U.S. District Court for
the Northern District of California against major motion picture studio
copyright holders (MGM Studios, Inc.) for a declaratory judgment that the
sales of its DVD copy software did not violate the DMCA.127

321 Studios argued the DMCA was unconstitutional as a restriction on
free speech and that “making personal backup copies of DVDs is expressly
authorized under the copyright laws as fair use.”128 The court held that under
an intermediate scrutiny standard that the DMCA did not impermissibly
burden 321’s First Amendment rights.129 In refuting the fair use argument, the
court further held that “…Fair use is still possible under the DMCA, although
such copying will not be as easy, as exact, or as digitally manipulable as
plaintiff desires.”130

The court granted the copyright holders summary judgment enjoining
321 Studios from manufacturing, distributing, or otherwise trafficking in any
type of DVD protection circumvention software, effectively shutting down the
company’s sales.131 One month after the Northern District of California
upheld an injunction against 321 Studios, the Southern District of New York
granted a similar injunction brought by Paramount Pictures and other movie
studios to prevent 321 Studios from selling DVD copy protection
circumvention software as violative of the DMCA.132 The court held that the
“DVD X Copy” series of applications violated the “anti-trafficking”
provisions of 17 U.S.C. § 1201(a)(2), § 1201(b)(1) in providing software
primarily marketed to the public as a way to circumvent CSS, with secondary
capability to restore damaged DVDs.133 Later in 2004, 321 Studios shut down
completely.134

2004); See also, Lisa Rein, Fair Use vs. DMCA: 321 Studios Takes the First
Swing, O’REILLY DIGITAL MEDIA, April 23,2002,
_studios_t.html.
129 Id. at 1100 (citing Turner Broad. Sys., Inc. v. FCC, 512 U.S. at 624).
130 Id. at 1102.
131 Id. at 1105.
132 Paramount Pictures Corp. v. 321 Studios, No. 03-CV-8970, 2004 WL
402756 (S.D. N.Y. 2004).
133 Id.
134 Katie Dean, 321 Studios Shuts Its Doors, WIRED NEWS, Aug. 4, 2004,
Oddly, consumers who go to the 321 Studios Web site will see advertisements for a new “DVD-X Copy” software that claims to “Make Perfect Copies of Your DVD Movies.”\textsuperscript{135} The software includes “With RIPPER Pre banned Software SEALED RETAIL BOX.” A disclaimer at the bottom of the Web site states: “©2005 :: 321StudiosInc.com :: Policy :: We are in no way associated with the former 321 Studios or dvdxcopy.com.” Strangely, the new “321 Studios, Inc.,” selling “DVD X Copy” is not related to the former “321 Studios,” which sold “DVD X Copy” and was enjoined from selling software by two U.S. federal courts.

In spite of the advanced 40-bit CSS, Macrovision, Verance, CPRM, and DTCP copy protection, there is still a flourishing industry in software to copy DVDs. A simple web search comes up with plentiful sites selling DVD copy software.

The method to copy DVDs involves a combination of ripping, transcoding, removing data, shrinking data, or spitting data. Ripping is taking a DVD and copying the content (bypassing or eliminating the copy protection) to a computer. Trans-coding is taking the content and creating a sub-band or lower bit rate copy that will frequently eliminate the copy protection due to the generational loss. Removing, shrinking or spitting data is byte level manipulation of copy protection that bypasses encoded copy protection information.

Software such as “DVD Shrink,”\textsuperscript{136} “Any DVD”\textsuperscript{137} or “1Click DVD Copy”\textsuperscript{138} all accomplish the task. These software applications essentially perform a bit rate reduction from the master DVD MPEG-2 video to a lower bit rate that results in slightly inferior quality but removal of the encryption information. The newly ripped video will generally fit on a single layer DVD (~4.7 Gigabytes); differentiated from the dual-layer (~9.4 Gigabytes) DVD sold by stores for movie content. One such product will even instruct the user how to obtain a free third party DVD decrypter if it detects an encrypted disc!

The cases on DVD copyright protection measures are a window into the future of access to digital media. With developing online (Internet and cable VOD) access to television and movies at high definition resolution, the

broadcast and film industry has a very strong incentive to control access to content. The type of “fair use” by consumers will depend on the technology of content protection and the interpretation of the DMCA by the courts. The term “fair use” as it relates to Sony v. Universal, may become “allowable use” as a result of the DMCA § 1201.

At the Sundance Film Festival in January 2006, an independent film created by Kirby Dick called “This Film is Not Yet Rated” was illegally copied by the MPAA itself. The film is about the American movie ratings board and had not yet been released.139 The MPAA’s own lawyer even admitted to copying the DVD.140 Mr. Dick has sued to recover all illegal copies of the film and to determine who ordered the illegal copy.141 Apparently the MPAA ignored its own Web site’s warning, which states: “In 2005, President Bush signed the Family Entertainment and Copyright Act, which … establishes new penalties for pirating works that have not yet been released commercially. First-time violators can be sentenced to three and five years, respectively, for these crimes and fined up to $250,000.”142 It would be interesting if the MPAA’s own attorney were jailed for DVD piracy.

III
TELEVISION AND MOVIES

A. In General

In the United States, over-the-air television is a combination of the traditional National Television Standards Committee (NTSC) standard codified under Society of Motion Picture and Television Engineers standard SMPTE-170M analog broadcasting with a government-mandated migration to Advanced Television Standards Committee (ATSC) A/53 digital broadcast channels by February 17, 2009.143 The analog NTSC standard was adopted in 1941 and amended in 1953 to add the RCA electronic color system.144 The NTSC standard has often pejoratively been called “Never Twice the Same

139 THIS FILM IS NOT YET RATED (Independent Film Channel 2006)
141 Id.
Color” due to early color reproduction problems. U.S. analog broadcasting has 525 lines of Standard Definition (SD) interlace scan video in a 4x3 aspect ratio (1.3:1). Analog television is subject to ghosts, static, noise and color alignment problems.

The ATSC digital television standard was adopted by the FCC on December 24, 1996, and specifies digital broadcasting in the same 6 MHz channel slot that an analog broadcast channel currently occupies in the electromagnetic spectrum. The ATSC standard provides for High Definition (HD) broadcasting comprising 720 progressive or 1080 interlaced lines of resolution in a 16x9 (1.7:1) aspect ratio using MPEG-2 compression at a nominal 19.39 Mbit/s effective data rate, including the capacity to carry a number of SD channels. Digital broadcasting is generally viewable or not. Digital broadcasting compensates for some noise, however excessive signal quality problems in a digital broadcast cause hits and freezes and will render a program un-viewable to most consumers.

Cable television generally contains at least some analog channels preserved in the original broadcast standard format to accommodate viewers with legacy set-top boxes (STB), along with a large number of compressed SD channels. Most major cable systems such as Time Warner, Comcast, and Cablevision advertise support for digital cable relying universally on the MPEG-2 digital video compression standard.

Direct broadcast satellite (DBS) transmits all channels using MPEG-2 digital compression at variable bit rates, with DirecTV moving to MPEG-4/AVC to accommodate HD content.

Cable television uses a key within the set-top box to control content. As a result of the keyed system, cable providers can easily enable or disable services in set-top boxes with great control. Although many Web sites sell

---

148 Robert Heron, *DirecTV's HD Future is MPEG-4*, PC MAGAZINE, Jan. 6, 2005, http://www.pcmag.com/article2/0,1759,1748991,00.asp.
pirated descramblers and coaxial adapters, very few of these devices work properly in modern digital cable systems. CableLabs, the cable industry research company, manages specifications for DOCSIS, PacketCable, CableHome, and OpenCable standards that require embedding digital certificates in hardware set-top boxes when manufactured.

Cable VOD specifies MPEG-2 compressed content at 3.4 Mbit/s for Standard Definition or 19 Mbit/s for High Definition content. U.S.-based cable VOD does not currently use a TCP/IP based protocol for delivery.

Consumers generally already have on demand availability with digital cable on Time Warner, Comcast, Adelphia, and Cablevision if subscribing to digital cable. The nation's second-largest cable operator has initiated talks with the four biggest broadcast networks — CBS, ABC, Fox and NBC — about testing a service that would give viewers “on demand” access to top programs, as rated by Nielsen Media Research, soon after their broadcast.

CBS and Comcast began offering video on demand services in January 2006 (including shows such as CSI: Crime Scene Investigation, NCIS, Survivor and The Amazing Race) available after midnight on the nights the original shows air on the network. Cable on demand generally provides access to content for twenty-four hours from the time of purchase for a few dollars.

---

152 Richard Siklos, Cable Negotiates to Offer Instant Reruns (for a Fee), N.Y. TIMES, Mar. 27, 2006, at C10.
Satellite television uses CA technology to control access to content relying on technologies such as VideoCipher, DigitalCipher, VideoGuard, Conax, Cryptoworks, Irdeto, Mediaguard, Nagravision, and Viaccess. Consumers have largely migrated to Direct Broadcast Satellite services after imposition of strong encryption on most network satellite feeds.

Direct Broadcast Satellite (DBS) has long been the target of copyright pirates, due to the open-air signal and difficulty of getting caught. DirecTV, with over fifteen million paying customers, has had a rich history of piracy. DirecTV uses standard ISO-7816 smart cards for Conditional Access, which has been repeatedly cracked. The introduction of P4 smart cards in 2002 and new D1 and D2 smart cards in 2005 has slowed DirecTV piracy, but not stopped it. By 2004, DirecTV had filed lawsuits against 24,000 people claiming damages starting at $3,500 and up for piracy under the authority of the DMCA. Even OJ Simpson was sued for $25,000 in 2005 for pirating DirecTV. DirecTV operates a Web site to inform users about satellite fraud and piracy.

In a strange twist in 2002, Paris, France based Canal+ sued Haifa, Israel-based NDS (a division of News Corp., owner of DirecTV) for stealing its digital TV Smart Card code (UserROM) for Conditional Access (CA). The suit, filed in the Central District of California, alleged unfair competition, copyright infringement, violation of the DMCA, tortious interference,

---

conspiracy and violation of the Racketeer Influenced and Corrupt Organizations Act.\textsuperscript{163} Canal+ sought more than $1 billion in damages. The case was settled out of court in 2002 in a deal between Canal+ parent Vivendi and News Corp.\textsuperscript{164}

Movies are still largely shot and distributed on 35 mm film, generally at 2.3:1 aspect ratio (cinemascope) at 24 frames per second (fps), with each frame repeated twice for an actual frame rate of 48 fps. Beginning with \textit{Star Wars: Episode II}, George Lucas made cinematic history by shooting a major motion picture entirely with Sony HDC-900 High Definition 24-frame progressive scan video cameras, and not with traditional film.\textsuperscript{165} This key change enables easier digital video effects rendering, and simplifies distribution to theaters as digital files for digital projection.\textsuperscript{166} Digital projection abolishes film dirt and eliminates jitter and weave by the projector shutter.\textsuperscript{167} Digital television and digital movies can be distributed and managed on videotape or as files; however, digital rights management (DRM) is a primary concern. In February 2006, the Philips CineFence digital watermarking technology was selected by Access Interactive Technologies (AccessIT) for use in digital cinema file distribution to Christie/AIX equipment in movie theatres.\textsuperscript{168} It is unclear whether CineFence will protect against a person sitting in a theatre with a camcorder, or whether the recorded content will still contain the watermark.

According to one study, the movie piracy often attributed to people in movie theatres or on the street is actually more likely to come from industry

\begin{quote}
\textsuperscript{163} John Cassy & Paul Murphy, \textit{How Codebreakers Cracked the Secrets of the Smart Card}, \textsc{The Guardian}, Mar. 13, 2002, at 3.
\end{quote}
According to an AT&T study in 2003, 77 percent of all pirated files come from industry insiders. Thus despite the headlines from the MPAA of how copyright infringement is supporting terrorism, it appears that the source of the problem is mainly the motion picture industry itself. Bad internal security policies are the primary culprit. According to the report:

Our study shows a large amount of insider leakage. Hence, we argue that current mitigation techniques are insufficient. Given the revenue losses claimed by the industry, spending more money and effort on internal controls is appropriate. Movie artifacts are handled by a limited number of employees in a controlled manner during production and through much of the distribution process. In the later stages of distribution, content is handled by a large and mostly anonymous community. Securing the former environment is difficult but tractable. Securing the latter is nearly impossible. Hence, focusing efforts on insider threats addresses the most costly leakage, and represents the best opportunity for success.

Clearly the industry itself must bear some burden for preventing file-based content from becoming available to the masses.

If the majority of piracy is coming from within the studios, clearly someone “inside” is profiting from the theft. Could there be a link between legitimate movie studios making illegal income from vicarious copyright infringement? This seems doubtful. However, if so, the implications would be far reaching. Vicarious liability requires: (1) the right and ability to supervise or control the infringing activity; and (2) a direct financial benefit from that activity.

In Shapiro, Bernstein & Co. v. H.L. Green Co., where the owner of twenty-three stores hired a direct copyright infringer to operate the record

---

171 Id. at 11.
departments, the court explained vicarious liability as: “[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials … the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation.” 172

Movies, television and music are distributable as streams or files over cable systems, over the Internet or via mobile (phone) terrestrial networks. The quality ranges from a postage stamp size window at 56 kBit/s, to full bandwidth high definition at 1.5 Gbit/s. Between a downloadable file, and a stream-able file there are key differences in content protection technology.

With analog NTSC over-the-air television broadcasting, there is little viable content protection. Audio watermarking with Verance technology is commonly used to confirm that proper content was aired, but it cannot block viewers or control access. 173 Philips has developed “Teletrax” audio and video watermarking and fingerprinting, however there is little benefit to widespread protection of analog over-the-air television. 174 Mostly this technology is used to confirm that advertisements were properly aired. The key value to both Verance and Philips (Teletrax) technology will be for high definition television. Philips claims that the watermarking technology developed will survive when high definition content is compressed down to Internet stream-able file sizes using DIVX and MPEG-4. 175

B. The Broadcast Flag

The Broadcast Flag would have been a set of bits in a digital television signal that define the user rights to specific content, such as whether it may be recorded, and if so how many times. 176 In 2002, Mel Karmazin, then at

173 See Verance, supra note 102.
176 Am. Library Ass’n v. FCC (ALA II), 406 F.3d 689, 691 (D.C. Cir. 2005) rev’g in part, vacating in part Am. Library Ass’n v. FCC (ALA I), 401 F.3d. 489 (D.C. Cir. 2005).
Viacom, made a public threat to pull CBS high definition broadcasting off the air in the 2003-2004 broadcast television season without a broadcast flag.\(^{177}\) Other major networks had made similar complaints about broadcasting high definition television without adequate copyright protection. On November 4, 2003, despite enormous criticism of a Notice of Proposed Rule Making in 2002,\(^{178}\) the FCC passed a rule requiring a Broadcast Flag to be included in any digital broadcast reception equipment.\(^{179}\) The rule was in response to pressure from the television and film industry and included the following language: “No party shall sell or distribute in interstate commerce a Covered Demodulator Product that does not comply with the Demodulator Compliance Requirements and Demodulator Robustness Requirements.”\(^{180}\)

The rule would have taken effect in 2005. In response to the FCC rule, a group of five library associations along with public interest groups filed suit in the D.C. Court of Appeals, claiming that the FCC had acted outside its authority in passing the Broadcast Flag rule.\(^{181}\)

The principal question in *American Library Association v. FCC* according to Circuit Judge Edwards was whether, under the Communications Act of 1934, Congress delegated authority to the FCC to “regulate [an] apparatus that can receive television broadcasts when those devices are not engaged in the process of receiving a broadcast.”\(^{182}\) In the first sentence of the opinion the court starkly noted that “[i]n the seven decades of its existence, the FCC has never before asserted such sweeping authority.”\(^{183}\)

The FCC claimed authority for the rule under Title I of the Communications Act of 1934.\(^{184}\) In a 3-0 ruling, the court held that the FCC


\(^{180}\) Digital Broadcast Television Redistribution Control, 47 C.F.R. § 73.9002(b) (2006).

\(^{181}\) *ALA I*, 401 F.3d at 489.

\(^{182}\) *ALA II*, 406 F.3d at 691 (citing 47 U.S.C. § 151 (2000)).

\(^{183}\) *Id.*

\(^{184}\) 47 U.S.C. § 151 (2000) (creating the FCC “for the purpose of regulating
had no authority to regulate consumer devices “that can be used for receipt of
wire or radio communication when those devices are not engaged in the
process of radio or wire transmission.” This effectively stated that because
devices may be used for purposes other than broadcast reception, the FCC had
no right to regulate the use.

After the court defeat, during Senate Commerce Committee hearings
on January 24, 2006, the Broadcast Flag was dealt an even stronger blow. In
response to a statement that a lack of Broadcast Flag will stifle creativity
and innovation, Senator John Sununu of New Hampshire stated:

The suggestion is that if we don't do this, it will stifle creativity. Well...we have now an unprecedented wave of
creativity and product and content development...new business
models, and new methodologies for distributing this content. The
history of government mandates that it always restricts innovation: why would we think that this one special time, we
are going to impose a statutory government mandate on technology, and it will actually encourage innovation?

Senator Ted Stevens of Alaska later asked whether an audio Broadcast
Flag would potentially restrict recording of radio programs to put onto his
iPod, to which Mitch Brainwol of the RIAA answered that it would.

The status of the Broadcast Flag is uncertain with a major court defeat
and little support in Congress. Viacom never pulled any CBS high definition
television from the airwaves. The television and film industry is in a
precarious position. There has been no specific congressional restriction on
copy protection technology in consumer electronics, only displeasure with
government mandated content protection.

interstate and foreign commerce in communication by wire and radio…”).

185 ALA I, 406 F.3d. at 699.
186 Danny O’Brien, History and Senator Stevens iPod, ELECTRONIC FRONTIER
FOUNDATION, Jan. 25, 2006, http://www.eff.org/deeplinks/archives/004343.php; See also Boing Boing,
Senators Figure Out the Broadcast Flag, Curse it to Abomination,
http://www.Boingboing.net/2006/01/28/senators_figure_out_.html (last visited
Mar. 5, 2007).
187 Alex Curtis, Broadcast Flags Hearing Recap, PUBLIC KNOWLEDGE, Jan.
188 O'Brien, supra note 186.
IV
HIGH DEFINITION COPY PROTECTION

After the DTCP-5C work was completed, Digital Content Protection, LLC (a subsidiary of Intel based in Hillsboro, Oregon) created the High-bandwidth Digital Content Protection (HDCP) system specifically to address the High Definition Multimedia Interface (HDMI) and Digital Video Interface (DVI) connections used for high definition television.\(^{189}\) HDCP is the next generation of DTCP. HDCP licensing costs an annual fee of fifteen thousand dollars (US $15,000) plus a per unit fee of: $0.005 per "device key" purchased (to enable encryption/decryption).\(^{190}\) HDCP provides a secure channel between the set top box and the television that must be triggered by a Conditional Access instruction. Whereas today the connection from the cable box to the television is generally an analog coaxial modulated signal, in the future with digital broadcasting, the connection is likely to be HDMI or DVI with HDCP required. The consumer has no control over when HDCP content protection is used or how it is used.\(^{191}\) HDCP does not work for over the air broadcasting due to the short duration of time required for exchange of cryptographic key pairs between the source and destination devices.

In 2001, Niels Ferguson, a Dutch cryptographer, hacked the HDCP.\(^{192}\) However, Mr. Ferguson did not publish his results for fear of prosecution under the DMCA.\(^{193}\) After the arrest of Russian programmer Dmitry Sklyarov under §1201(b)(1)(A) of the DMCA for cracking the Adobe eBook rights management, foreign developers are increasingly hesitant to publish cryptographic work or to enter the United States.\(^{194}\)

---


\(^{190}\) 5C DIGITAL TRANSMISSION, supra note 91.


\(^{193}\) Id.

\(^{194}\) Dmitry Sklyarov was arrested in Las Vegas on July 16, 2001 under the DMCA. Dmitry and his company ElcomSoft Co., Ltd. were indicted by a grand jury of circumvention offenses and aiding and abetting circumvention offenses, under the DMCA, and a charge of conspiracy to traffic in a circumvention program. Dmitry was released in December 2001 and allowed to return to Russia under an agreement to testify against his employer,
DVI is one of two connector types supported on high definition television sets. Today, both major satellite providers require HDCP over DVI from set top boxes for high definition television. DVI carries video only. One confusing issue is which of the five different flavors of DVI is to become prevalent: DVI-I (Digital & Analog) Single Link, DVI-I (Digital & Analog) Dual Link, DVI-D (DVI Digital) Single Link, DVI-D (DVI Digital) Dual Link, and DVI-A (DVI Analog) all have subtly different connectors that the consumer would be hard pressed to identify or understand.

Whereas DVI only carries video, the second connector type, HDMI, carries both audio and video unlike DVI. The general trend among manufacturers is towards HDMI with HDCP however both DVI and HDMI formats are common. The consumer electronics industry has done a spectacular job of thoroughly confusing consumers with the interconnection technology and the copy protection to be used for high definition television. There is only one type of HDMI, but it is very different from DVI.

Both HDMI and DVI are intended to plug the popularly referenced analog hole. The “analog hole” describes the problem that upon conversion from digital back to analog video all copy protection is lost and content becomes easy to steal.

One proposal for HDMI and DVI that is guaranteed to irritate consumers is the use of an Image Constraint Token (ICT). ICT is bits in the Advanced Access Content System (AACS) encryption that would down-convert quality through analog outputs rather than eliminate the video altogether. For example, this would result in taking high definition television

---

196 Id.
197 Id.
199 Weatherhead, supra note 195.
Developed by Toshiba, the HD-DVD uses a blue laser to store 30
Gigabytes of data on a standard dual layer disc. According to Toshiba, a
future triple layer disc will hold up to 45 Gigabytes. This capacity will allow
for storing a full-length high definition movie encoded at 30 Megabit/second.
The HD-DVD is backwardly compatible with today’s DVD players. The
introduction of the HD-DVD has been delayed from late 2005 due to DRM
issues.

Not to follow another standard, Sony Electronics created the Blu-Ray
Disc. The Blu-ray Disc can store 25 Gigabytes (single layer) or 50
Gigabytes (dual layer) on a single-sided disc — about five to ten times the
capacity of a DVD allowing for a full length feature on a dual layer disc at 40
Megabit/sec. Both use the same 405nm wavelength blue-violet laser but
due to differing track pitch and aperture the formats are incompatible.

A consortium of IBM, Intel, Microsoft, Matsushita, Sony, Toshiba,
Walt Disney and Warner Bros. Studios formed the Advanced Access Content
System Licensing Administrator (AACS LA) to develop and license AACS

201 Eric Bangeman, *HD DVD and Blu-Ray Content to be Degraded for Analog
Displays*, ARS TECNICA, Jan. 22, 2006,
http://arstechnica.com/news.ars/post/20060122-6027.html. See also, HDTV
Digital Home, What is an Image Constraint Token?,
http://www.digitalhomecanada.com/hdtv/idx/0/414/article/What_is_an_Image

202 Yoshiko Hara, *Toshiba Delays HD DVD Player Intro in Japan*,
ELECTRONIC ENGINEERING TIMES, Dec. 13, 2005,
cleID=175000947.

2007).

204 For a comparison of the various features of HD-DVD and Blu-Ray see
CNET, Blue-Ray, *HD-DVD and DVD Formats Compared*,
http://reviews.cnet.com/4520-6463_7-6462511-2.html (last visited Mar. 5,
2007).

the-s-union-s-division.
technology for HD-DVD and Blu-Ray. AACS is effectively the next generation of CSS. Unlike the weak 40-bit encryption in CSS, the proposed AACS standard will use a 128-bit Advanced Encryption Standard as specified by the U.S. National Institute of Standards and Technology (NIST) in Special Publication 800-38A. According to IBM, the AACS technology has been available for licensing since of February 2006. The AACS LA was designed to avoid another embarrassing experience with a Norwegian teenager like Jon Johansen. However, on January 15, 2007 an anonymous Hacker known as Muslix64 publicly distributed the movie Serenity, which was ripped from an HD-DVD using freeware called BackupHDDVD to show the industry that the AACS standard had now been officially hacked. Muslix64 used the ever-popular BitTorrent to distribute the ripped movie.

Further, both HD-DVD and Blu-Ray will only work with HDMI or DVI outputs, which have built in copy protection via HDCP and DTCP. To date, most players only have HDMI outputs for high definition content. If a consumer has an older (more than 3 years) television capable of high definition display, it is unlikely to have a DVI or HDMI input and will be useless for HD-DVD, DVI, or even for most new set top boxes.

Verance technology is included in the AACS for content management. Macrovision has not been included in the AACS standard; however it will still support analog ACP for analog outputs where appropriate. The problem is that the industry is moving to completely eliminate support for analog outputs. In fact, it is beginning to feel like high definition accommodates little “fair use.”

To summarize current high definition copy protection, watermarking is tracking (protection) for live or recorded content, AACS is protection for

---

212 Id.
prerecorded content on the disc itself and HDCP is a device (player) to display (television) protection (over HDMI and DVI).

The defeat of the Broadcast Flag means that currently, consumers may watch and potentially record high definition television and movies over the air with impunity. The ATSC standard has no suite of DRM tools. The lack of DRM in the ATSC standard has created tension between copyright holders, consumers, the government and manufacturers.

It appears that the industry is at a Sony moment and may determine whether consumer time shifting as “fair use” still exists. The combination of HDCP, HDMI and AACS will address head-on Justice Blackmun’s concern in Sony about library building.

V

STREAMING AND FILE BASED DELIVERY

The number of content encoding standards and storage formats for file-based video is dizzying. Commonly seen formats for digital file based content include: Moving Picture Experts Group – MPEG-1, MPEG-2, MPEG-4 (Advanced Video Codec or H.264), AVI, ASF, WindowsMedia (VC-1, SMPTE 421M-2006),213 Apple QuickTime, RealVideo, Google Video, Macromedia Flash, DV25/50, HDV, and many others.

DRM and copy protection applies on a case-by-case basis depending on the type of encoding, compression, lines of resolution, and vendor support. A great web of complexity results when a matrix is created including copy protection technology, overlaid with digital media encoding schemes. Unfortunately for consumers, this will only become more complex with the arrival of new formats and digital broadcasting.

After a wildly successful Victoria’s Secret fashion show was streamed live in 1999, Yahoo! purchased Broadcast.com for $5.9 billion and Yahoo! created Yahoo! Broadcast.214 Ultimately, Yahoo! Broadcast has disappeared as an independent service, apparently leaving Yahoo! with no direct to

---

213 SMPTE Releases VC-1 Standard, MEDIALINE, Apr. 6, 2002, at 36.
consumer video store. Yahoo! has a videos section that operates as a Web search for posted videos. Apparently, $5.9 billion does not buy a viable online-video store.

In April 2005, Google created Google Video. The Google Video store provides downloads of some free content and sales of some network television content. Current CBS television network programs are available on Google Video for $1.99 a show without commercials and without channel branding bugs or snipes. Google uses rebranded GVI files (essentially DivX4 encoded .AVI files with MP3 audio). The shows are protected with yet another DRM scheme that is incompatible with Apple FairPlay or Microsoft DRM. Currently TV shows purchased on Google Video (from CBS) do not include commercials. It is not certain whether this will last. It is possible that advertising by product placement may supplant lost revenue due to a lack of ads in downloadable programs, however a recent study by FIND/SVP suggests that product placement is not nearly as effective as traditional television advertising.

Apple released the iTunes media player, essentially rebranding the “SoundJam MP” from Casady and Green in January 2001. The iTunes software coincided with the release of the iPod portable music player with 5GB of storage. Apple added iTunes for Microsoft Windows in October 2003, with video support in May 2005. In November 2005, Apple released

---

218 According to the FIND/SVP study, only 23 percent of those asked said they would consider purchasing a product from a product placement advertisement, where 52 percent were inclined to purchase after viewing a traditional advertisement. See Wayne Friedman, Study Finds Ads More Persuasive Than Product Placement, Media Daily News, Aug 22, 2005, http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=33347.
221 Wikipedia, iTunes, supra note 219.
a video capable iPod with a 3.5” diagonal 4x3 screen and announced that episodes of ABC series Lost and Desperate Housewives would be available for download for $1.99 per episode the day after broadcast. Content purchased on iTunes uses “FairPlay” DRM that allows up to five computers to play the file, upon proper authorization. Ironically, at a 2003 investor conference, Steve Jobs admitted that Apple makes no profit from the iTunes music store, rather, all the revenue comes from the sales of iPods. Apparently the copyright holder record companies reap all the profits.

iTunes “FairPlay” has been repeatedly hacked. In 2004, even RealNetworks hacked FairPlay (discussed infra). In 2005, a group of programmers (including the infamous Jon Johansen who cracked CSS) created PyMusique as an iTunes music store client to strip Apple’s DRM. The next business day Apple plugged a hole in its server to squash PyMusique, and the following day the same programmers found a new hole and released an updated version of PyMusique. In 2005 Jon Johansen

---

223 iTunes Support, http://www.apple.com/support/itunes/musicstore/authorization/ (last visited Mar. 5, 2007). Note: In a recent article, Apple CEO Steve Jobs wrote that “DRMs haven’t worked, and may never work, to halt music piracy.” This article suggests that DRM-free music sales would be a viable alternative if only Universal, Sony BMG, Warner and EMI – who control 70 percent of music distribution across the globe – would agree to remove the DRM system requirements. This article has elicited many responses from all corners of the entertainment industry ranging praise and agreement to outrage and criticism. Steve Jobs, Thoughts on Music, Feb. 6, 2007, http://www.apple.com/hotnews/thoughtsonmusic/.
228 See Rosenblatt, supra note 225.
abandoned PyMusique to create SharpeMusique as the next revision of the iTunes music store interface.\textsuperscript{229} Apple has not filed any lawsuits against the creators of PyMusique or SharpeMusique.

NBC Universal has begun to distribute at least eleven series on the web through Apple iTunes.\textsuperscript{230} Shows such as The Office and Scrubs will be complimented by retro series like Dragnet all for $1.99 an episode. One undesired consequence of direct sales of television programs on iTunes and Google, has been loud complaints by television network affiliates on loss of advertising revenue.\textsuperscript{231} The affiliates are clearly concerned and some have even said that the writing is on the wall for networks to accept a bit of “forced evolution” as a result of online and on-demand video.\textsuperscript{232}

BitTorrent is a protocol for high speed file copy specifically targeted at video and audio content. Originally developed by San Francisco programmer Bram Cohen, and presented at DefCon in Las Vegas in 2001, BitTorrent has been largely used for illegally sharing games, television shows and movies over the Internet.\textsuperscript{233} In 2004, the MPAA initiated suit against BitTorrent sites ultimately shutting down the bulk of illegal file sharing sites.\textsuperscript{234} In 2004, CacheLogic estimated that thirty percent of all Internet traffic was from BitTorrent.\textsuperscript{235}

In one particularly riveting episode, the MPAA sued one of the most popular BitTorrent sites on the public Internet, LokiTorrent, for contributory copyright infringement. The site was serving over 680,000 active members. However, after the site owner, Edward Webber, collected $40,000 in donations to fight the lawsuit, he capitulated and turned over all the server logs, including user information, to the MPAA. These server logs were ostensibly for use in further copyright infringement lawsuits. In an ironic twist, on May 9, 2006, Warner Brothers announced that movies and television programs would be available over the Internet for download using BitTorrent with copy protection licenses. Warner Brothers chose BitTorrent because it was “elegantly and efficiently designed for the delivery of large files like TV programs and films.”

In 2005, on the heels of Grokster, San Mateo based SlingMedia created the “Slingbox.” The Slingbox is a small electronic “brick” that sits on the top of a television set and allows users with a broadband connection to stream live broadcasting to anywhere on the Internet. This $250 box provides technology called “place shifting” with no subscription fees. Slingbox does not allow file sharing and only permits streaming to one destination at a time. The founder of SlingMedia, Blake Krikorian, sees Slingbox as a way for consumers to gain access to local television programming via the Internet while at work or away from home.

Regarding the Slingbox and place shifting, Martin Franks of CBS stated in 2005 that, “Slingbox is one manifestation of what we assume will be a cascade of similar products that are meant to manipulate our signals in ways that we think will be harmful to the network-affiliate business, if not the law.”

Richard Parsons of Time Warner also commented on the Slingbox technology saying, “I can’t guarantee that there aren’t going to be any lawsuits because there probably are . . . . Technology, rights management, and consumer behavior don’t necessarily move in lock-step.”

Orb Networks, Inc of Emeryville, California sells a similar software-only product that allows users to stream live television, photos, audio, or stored video to anywhere on the Internet. Ted Shelton, the CEO of Orb Networks, admitted that it is likely a case involving Orb Networks or Sling Media will end up at the Supreme Court sometime in the next decade. The law is unsettled on whether consumers have the right to place shift under the time-shifting “fair use” exception established by Sony. There is no clear information on how Orb Networks and Sling Media handle copyright protection, such as Macrovision or CGMS-A, if at all. It appears that there have been no court challenges from either the MPAA or broadcasters.

TiVo, an Alviso, California based corporation, was founded in 1997 and quickly became a household name for the Digital Video Recorder (DVR). TiVo or cable supplied DVR owners can record content as it is broadcast for future viewing until space runs out on the hard drive. The cable service costs around ten dollars per month. Based on cost alone, TiVo appears to be a better deal for the avid viewer due to user control, but it requires scheduling in advance. Cable video on demand generally subjects viewers to Macrovision content protection, which prevents TiVo local storage and disallows making subsequent analog copies by introducing visible noise.

TiVo sells subscription service for about seventeen dollars per month. This service provides a VCR replacement using a built in hard drive to digitize video. The box runs on a Linux operating system with a built in MPEG-2 video encoder/decoder, and includes an easy to use software

---

242 Id.
244 Wallenstein, supra note 241.
interface independent of the cable-system or satellite provider used. TiVo has some built in TiVoGuard Digital Output Protection Technology native to the box for protection of content from copying. However, this does not patch the “analog hole” that allows a consumer to record from TiVo to a VCR or DVD-Writable. Other technology such as DTCP, HDCP, or Macrovision is required.

TiVo gained some notoriety in 2004 when it reported that the most TiVo’d event in history was Janet Jackson’s “wardrobe malfunction” during the Super Bowl in January.\(^{247}\)

TiVo would appear to be ripe for peer-to-peer file sharing and copyright infringement. In 2004, after TiVo publicly announced plans for “TiVoToGo” to allow sharing of recorded files, the MPAA and the NFL filed a petition with the FCC to block the release of the service.\(^{248}\) The MPAA and the NFL argued that copyrighted content could be released on the Internet. In response TiVo applied to the FCC for permission to sell the ToGo service with safeguards for content protection.\(^{249}\) After the FCC granted permission to TiVo in August 2004, Tivo released TiVoToGo in 2005, which remains on the market apparently without any direct court challenges by the MPAA or the NFL.\(^{250}\)

On its Web site TiVo discusses the legality of TiVoToGo:

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>“Are TiVoToGo™ transfers legal?”</th>
</tr>
</thead>
</table>
| ANSWER   | “Yes, TiVoToGo transfers are legal when used as intended by TiVo Inc. The TiVoToGo feature of the TiVo service is provided for your personal, non-commercial use. TiVo has taken deliberate steps to protect the content that originates on our digital video recorder and is transferred to the PC via our TiVoToGo feature…. Distribution and/or use of such tools to transfer copyrighted works outside of your home


Another popular independent personal video recorder (PVR), ReplayTV, formerly from SONICblue, included a handy thirty second ad-skipping feature. Obviously, this was unpopular with the broadcast industry, and the major networks sued SONICblue. However, in the midst of a 2001 lawsuit by the major U.S. television networks, ReplayTV declared bankruptcy. D&M Holdings, owner of Denon and Marantz, based in Tokyo, Japan, purchased Replay. A new ReplayTV box has emerged with the removal of the ad-skipping feature.

Internet protocol television (IPTV) is the encapsulation of encoded digital video into internet protocol packets for transmission over data networks. It generally is classified as streaming video; however, streaming carries the connotation of postage stamp sized images with poor quality audio. The term IPTV may describe live video streaming, stored video streaming, and download of video for time shifting or store and carry to portable devices. Internet protocol technically describes the network layer (layer 3) in the 7-layer Open Systems Interconnect (OSI) model. International Standards Organization (ISO) developed the OSI model to assist in defining protocol interconnection for data networks. The current version, IPv4, relies on 32-bit addresses in an architecture that allows packets to travel over heterogeneous networks.

IP was not designed for video; it was designed for multiple users over dissimilar data networks. Ethernet was not designed for video; it was designed for multiple users over contentious (shared) data networks. However, the Internet and Ethernet networks are ubiquitous and can be augmented for video delivery at reasonably high data rates with the proper design. The two transport protocols (layer four of the OSI model) for delivery of IP packets are

---

User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). UDP is unidirectional, connectionless and preferred for IPTV. TCP requires bi-directional communication and confirmation of packet delivery. TCP is generally unusable for IPTV due to the negative impact on video quality of retransmissions.

Technical issues notwithstanding, IPTV has broken the mold from a novelty to a viable mechanism for watching video. Microsoft has been moving rapidly into IPTV with sales of high quality encoding and presentation software. Other reputable traditional companies such as PanAmSat are seriously looking at delivering content over IP networks.

The evolution of IPTV has had some bumps. In 2004, Microsoft and, Swisscom telecom subsidiary, BlueWin began a highly touted pilot to test Microsoft TV in 600 homes in Switzerland with an expected rollout to 200,000 homes. In late 2005, BlueWin was forced to delay the rollout of the Microsoft TV system because according to Swisscom, “it has become apparent that the technology currently available is not yet suitable.” The status of BlueWin’s deployment at this point is unclear.

IPTV removes the tether to the local cable company or broadcaster and turns the entire Internet into a possible broadcast network. iTunes and Google Video are the beginnings of online delivery of programs. Fiber to the home provided by ATT/SBC with Lightspeed or Verizon with FiOS may provide the higher bandwidth required to provide watchable standard definition video. AT&T Lightspeed is intended to be an entirely IP based delivery system with fiber to the home. Verizon FiOS is already deploying a service

---

using two wavelengths of light; one to deliver IP based data (VOIP, Internet) and the other to deliver video using Quadrature Amplitude Modulation (QAM). ²⁶¹ Both services are advertised as capable of high data rate delivery, which will blur the lines between IPTV and traditional broadcasting.

Internet protocol delivery issues and higher bit rate required for high definition television will likely guarantee that broadcast technology will retain a quality edge over IPTV for the foreseeable future. Verizon is using Microsoft software to manage the FiOS service. ²⁶²

IP is merely a protocol for data delivery subject to all the copy protection data included in the payload. DRM in IPTV will depend on the format of video delivered and the display technology used to present it. Microsoft has ingeniously created an encoding standard (WM9) including rights management and all the tools to support IPTV, along with a founding membership in the AACS. ²⁶³ The public Internet is still problematic for video delivery, due to problems with reliable high speed data delivery. Although home users can get data at up to 2 Mbit/s on many cable modem or DSL based systems, the packet delivery is not guaranteed and susceptible to disruption due to activity by other users. ²⁶⁴ Until the deployment of Internet2 or high speed fiber to the home, video delivery will be limited. Other mechanisms such as WiMax, public WiFi, and power lines are still not substantially deployed to provide adequate bandwidth for large scale IPTV.

Despite technical hurdles, CBS recently was hugely successful with the on-line streaming of the NCAA “March Madness” 2006 college basketball on the Web. According to Larry Kramer, president of CBS Digital Media, there were over 200,000 people watching basketball on the Web at a given moment. ²⁶⁵

²⁶⁴ Microsoft TV, supra note 256.
RealNetworks Helix DRM is a secure content delivery mechanism for streaming media supporting RealAudio, RealVideo, MP3, MPEG-4, MPEG-2, AAC, H.263 and AMR. In 2004, RealNetworks wrote software called Harmony that effectively hacked Apple’s FairPlay DRM to allow Helix DRM encrypted files to play on the iPod. This occurred after Apple balked at a request from RealNetworks founder Rob Glaser to license FairPlay. Real’s campaign has not been a smashing success, prompting unexpected ire from many users. Apple has not filed a suit in the matter. There is likely a good argument that RealNetworks simply reverse engineered the FairPlay DRM, which would be permissible under the DMCA in the absence of a click wrap agreement, unlike the circumstances involved in creation of DeCSS by Jon Johansen.

RealNetworks has been streaming media for years since the 1995 introduction of the Real Audio Player. However, in an embarrassing moment in 1999, RealNetworks was sued for invasion of privacy, trespass, and unfair competition after admitting that its RealJukebox software on users’ desktops included a unique ID number and had been uploading consumer data on listening habits to RealNetworks servers. Shortly thereafter, Real was forced to update both the RealPlayer and RealJukebox to eliminate the unique ID and stop reporting user listening habits. Privacy is one area that will likely test the integrity of the entire rights management field. It is impossible to track keys for purchased content without a valid user ID, however, consumer privacy laws protect users in dozens of states against retention and tracking of consumer information. Clearly strong DRM is mutually exclusive

268 Naraine, supra note 226.
with consumer privacy. One concern raised during discussions on the
Broadcast Flag is that it may support privacy-invasive copy protection. The
intersection of consumer privacy with DRM is a ripe area for litigation.

Windows Media Digital Rights Management (WMDRM) from
Microsoft includes a suite of products:

- Windows Media Rights Manager (WMRM) SDK for packaging
  content and issuing licenses;
- Windows Media Format SDK (WMF SDK) for building Windows
  applications which support DRM and the Windows Media format;
- Windows Media DRM for Portable Devices (WMDRM-PD) for
  supporting offline playback on portable devices; and
- Windows Media DRM for Network Devices (WMDRM-ND) for
  streaming protected content to devices attached to a home
  network.

Like all copy protection, WMDRM has been cracked. Microsoft
patched the most recent 2005 hack, but, if history is an indication, Microsoft
DRM will be the prime target for frustrated hackers trying to watch IPTV with
Windows content protection. In 2001, Intertrust, a vendor of anti-piracy
software, sued Microsoft for patent infringement as a result of WindowsMedia
DRM. In 2004, Microsoft settled with Intertrust for $440 million including
a licensing agreement.

273 Comment from the Electronic Privacy Information Center on Notice of
Proposed Rulemaking, FCC 02-231 (Dec. 6, 2002) (on file with FCC),
available at
274 Microsoft.com, Platforms for Windows Media DRM,
275 Wolfgang Gruener, Windows Media DRM Cracked, TGDAILY.COM, Aug.
276 ComputerWeekly.com, Hackers Target IE Browser,
277 John Borland, Anti-Piracy Company Sues Microsoft, CNET NEWS.COM,
Released as a game player, the Sony PlayStation Portable (PSP) is capable of playing movies encoded onto UMD media using MPEG-4. Over fifteen million PSP’s have sold worldwide, creating a rich market for portable media. A recent update to the PSP software includes the ability to play copyright-protected video. However, Sony cautions that “that some content providers may charge fees for obtaining or using copyright-protected video…[and] downloadable copyright-protected video may not be available in all countries and regions.”

However, unlike the iPod with video, the Sony PSP has been disappointing for use as a movie player. Without a nicely tethered iTunes equivalent for the PSP, the device remains predominantly a game player. Content protection will likely not be so critical for the PSP due to the lack of strong consumer demand for television or movies on the PSP.

To complement consumer choices, mobile phone video is emerging as yet another distribution medium. MediaFlo by Qualcomm, Vcast by Verizon, and Modeo by Crown Castle are all viable mechanisms for delivery of mobile video. Because cell phones have limited viewing size and storage, DRM will be a low priority for the foreseeable future. However, when the mobile phone, the iPod, TiVo and the PSP all merge into a single device then mechanisms of DRM such as CA, DTCP, AACS, watermarking and Macrovision will become just as important as with other forms of digital media.

---

282 Id.
VI
CONCLUSION AND RECOMMENDATIONS

Within the next five years, mass media will likely become digital from end to end, including digital broadcasting, digital cable, streaming video, digital satellite, digital file delivery of movies to cinemas, HD-DVD or Blu-Ray sales to consumers, and digital downloads to portable devices or streamed to cell phones.

What will the user experience be like? Cable or satellite will be delivered with Conditional Access protection from the provider to a set top box with a DVI or HDMI interface that requires HDCP protection. HD-DVD/Blu-Ray players will require a DVI/HDMI output with HDCP and content on the discs will include AACS copy protection that may not play on an analog output. All content will likely include Verance or Philips watermarking technology that will survive multiple generations. IPTV delivered over fiber to the home or over a copper Internet connection will include DRM from Microsoft, Real, or Apple in addition to its own watermark and may include DTCP or HDCP. Any TiVo devices will likely require HDCP/DTCP over the DVI/HDMI outputs or a USB 2.0 or IEEE 1394 connection. Legacy VCR’s will likely be useless and DVD burners will include DTCP or HDCP protection to restrict copying. Every bit of the content protection described is legal and enforceable under the Digital Millennium Copyright Act §1201.

A copyright holder may change the type and scope of content protection without any say on the part of the consumer. The copyright holder may change the duration of time a clip may be played. A copyright holder using iTunes may disable the ability to play content on devices or restrict the licensing of content completely. Place shifting will likely be severely restricted if permitted at all. Sling would likely not survive a court challenge by major broadcasters.

The future sounds like consumers will have far more access to content, but with far fewer rights to use it. One area of concern that has been dormant is that of the antitrust implications of DRM. Where a small group of vendors, such as the AACS-LA or DTLA form a consortium that effectively controls the pricing for DRM technology in consumer electronics, one may find a contract, combination or conspiracy, as described under Section 1 of the Sherman Act. The Supreme Court has held that any horizontal agreement to fix maximum or minimum prices is per se unlawful. As in Arizona v.

Maricopa County Medical Society, it is irrelevant if the price fixing is for minimum or maximum prices. The AACS-LA sets uniform licensing costs for manufacturers and copyright holders. It is unlikely that a manufacturer would raise an antitrust claim to avoid paying licensing fees, given close relationships between manufacturers; however a court may consider whether the pro-competitive effects of HD-DVD or Blu-Ray DRM outweigh the anti-competitive effects.

It may be more appropriate to look at price fixing for DRM under the rule of reason approach. The Sherman Act was intended to prevent unreasonable restraints on trade. As in National Society of Professional Engineers v. United States, the court found an unreasonable restraint on trade under the Sherman Act §1 without any price fixing at all. In the case of the DTLA and the AACS-LA there is clear price fixing, however in order to uphold the DMCA and copyright law in general, uniformity in rights management technology is likely not unreasonable. If challenged, a court will probably uphold the blanket licensing agreements for DRM under the precedent set in BMI v. CBS, Inc. In BMI the court held that a blanket license is not a “naked restrain[t] of trade with no purpose except stifling of competition … but rather accompanies the integration of sales, monitoring, and enforcement against unauthorized copyright use, which would be difficult and expensive problems if left to individual users and copyright owners.”

Two perspectives on the outlook of content protection are evident:

1. **Consumer Perspective**: Consumers must be given the freedom to reasonably store and manage content locally. Overwhelmingly, burdensome protection will result in consumer’s resisting technical advances and stunting the growth of new markets. Apple iTunes has created a good balance of content rights protection and reasonable flexibility, which arguably has contributed to its success.

2. **Copyright Owners Perspective**: The consumer must accept a reasonable expectation of increased scrutiny of content use. Perfect digital duplication of high quality video cannot be permissible over

---

286 Id. at 347
287 Advanced Access Content Systems, supra note 207.
289 Id. at 681.
291 Id. at 2.
high-speed data networks without adequate protection. Copyright owners must exercise tight control over studio masters and high-resolution content. Consumer privacy must be managed carefully to adhere to applicable law.

Without a simple and effective means of digital dissemination of files and streams, revenue potential will be lost. However, without effective content control, piracy will be rampant and revenue will be lost.

Foreign governments’ respect for international intellectual property laws is essential for protection with respect to foreign DVD duplication services and foreign located Internet servers holding copyright content. Fortunately, DRM standards have received relatively uniform adoption due to the industry consortium approach in creating standards such as DTCP, HDCP and AACS.

A marriage of “TiVo” technology, wireless carriers, high quality compression, on-demand access, the Internet, high-speed networking and portable media players will complete the picture for ultimate consumer flexibility. All that will be necessary is available content. Copyright holders of television and movies will not miss this opportunity, but the content must be reasonably free to travel in order to keep the customer happy.