Macrovision Corporation
2830 De La Cruz Blvd.
Santa Clara, CA 95050

(408) 743-8600 Main
(408) 743-8610 Fax

VIA ELECTRONIC SUBMISSION

February 20, 2003

David O. Carson
Office of the General Counsel
U.S. Copyright Office, Library of Congress
P.O. Box 70400
Southwest Station
Washington, DC 20024-0400
Tel (202) 707-8380
Fax (202) 707-8366

THE LIBRARY OF CONGRESS
COPYRIGHT OFFICE
37 CFR Part 201 [Docket No. RM 2002-4]
Rulemaking on "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies"

Statement of Macrovision Corporation

William A. Krepick, President and CEO
Macrovision Corporation
Tel (408) 743-8600
Fax (408) 743-8610
Email: corp-info@macrovision.com

Jack Isaacs, Legal Counsel
Macrovision Corporation
Tel (408) 562-8411
Fax (408) 743-8610
Email: legal@macrovision.com

Comment numbers to which Macrovision is responding:

Comments 1-50

Classes of copyrighted works that original comments proposed to be exempted:

(1) literary works;
(2) musical works, including any accompanying words;
(3) dramatic works, including any accompanying music;
(4) pantomimes and choreographic works;
(5) pictorial, graphic, and sculptural works;
(6) motion pictures and other audiovisual works;
(7) sound recordings; and
(8) architectural works.

Brief summary of the arguments in opposition:

Macrovision Corporation's own experience in supplying copy protection and digital rights management technologies to the video, music, games and computer software industries supports our strong belief that security technologies do not stifle innovation and the full enjoyment of copyrighted material by consumers but instead encourage copyright owners to broadly distribute their content in order to fuel the growth of new markets. Although we do appreciate that some well intended individuals believe that the Digital Millennium Copyright Act may have some unintended consequences and should be continually reviewed and refined to achieve its initial goals, we believe that consumers have enjoyed unfettered access to digital copyrighted material by virtue of the advent of the peer-to-peer file sharing networks to the detriment of the copyright industries that are some of the United States largest exporters. Thus, there is no need to grant consumers any additional personal use rights that have not already been provided by law. Instead, Congress must continue to outlaw any circumvention devices, techniques, or Internet "hacks" that masquerade under the guise of fair use. Industry should be given the opportunity to set standards and develop solutions that adequately protect copyright. However, if industry fails to do so within a reasonable period of time, Congress should enact legislation that requires the implementation of certain technological solutions that help protect digital content from unauthorized copying and distribution.

Comments by William A. Krepick

On Behalf of Macrovision Corporation

Thank you for considering Macrovision Corporation's input for the upcoming Library of Congress Copyright Office Digital Millennium Copyright Act ("DMCA") rulemaking proceedings. Macrovision strongly supports the extension of the DMCA. The continuing introduction of new technologies that can be used to misappropriate copyrighted material has created an even greater urgency to permit the use of copy protection, digital rights management, and security technologies to limit access to copyrighted material according to publisher/content-owner defined rules. However, we do believe that any such restrictions should be implemented with the capability to allow certain personal use features by consumers. We make the distinction between personal use features and "fair use" rights because we understand that fair use is a concept that applies to legal defense against copyright laws violations; it does not apply to specific rights of consumers. We encourage Congress to carefully evaluate legislative proposals that attempt to define personal use of copyrighted content consistent with the reasonable expectations consumers may have with

respect to the use of purchased and licensed materials and the reasonable expectations that the content owners may have with respect to controlling their intellectual property.

Macrovision's own experience in supplying copy protection and digital rights management technologies to the video, music, games and computer software industries supports our strong belief that security technologies do not stifle innovation and the full enjoyment of copyrighted material by consumers but instead encourage copyright owners to broadly distribute their content in order to fuel the growth of new markets. One need only look at the spectacular success of the DVD product from both a content and hardware perspective to understand that strong copyright legislation encourages rather than stifles innovation. Although we do appreciate that some well intended individuals believe that the DMCA may have some unintended consequences and should be continually reviewed and refined to achieve its initial goals, we believe that consumers have enjoyed unfettered access to digital copyrighted material by virtue of the advent of the peer-to-peer file sharing networks to the detriment of the copyright industries that are some of the United States largest exporters. Thus, there is no need to grant consumers any additional personal use rights that have not already been provided by law. Instead, Congress must continue to outlaw any circumvention devices, techniques, or Internet "hacks" that masquerade under the guise of fair use. Industry should be given the opportunity to set standards and develop solutions that adequately protect copyright. However, if industry fails to do so within a reasonable period of time, Congress should enact legislation that requires the implementation of certain technological solutions that help protect digital content from unauthorized copying and distribution. One such technology that would prove to be important in this regard, and that is not yet accepted by the hardware community is digital watermarking. This type of technology is important because it protects content in both the digital and analog domain and would encourage copyright owners to support new markets and business models that will provide more choice to consumers on how they view and consume copyrighted materials.

As a leading intellectual property protection and digital rights management ("DRM") technology company, Macrovision is in a unique position in the neutral zone between the hardware community and the content owner community. Macrovision strongly supports the principles behind the anti-circumvention legislation pursuant to Section 1201 of the DMCA. The DMCA was enacted to promote creativity and innovation in the digital age while protecting the "rights" of the copyright owner, by extending traditional copyright protections into the digital domain. The DMCA was carefully crafted to achieve a balance between the need to prohibit unauthorized distribution of circumvention tools that can undermine copyright management or DRM technologies and the reasonable personal use rights of consumers who access or acquire music, movies, software and books in electronic format.

If anything, the need to reinforce the basic tenets of DMCA are even more urgent than when it was originally enacted. As Robert Holleyman, President and CEO of the Business Software Alliance, recently wrote:

> Since the DMCA was enacted, the number of Americans on the Internet has nearly doubled, from 70 million people to 137 million. The copyright industry has expanded at a rate of 10 percent each year. And, last year, copyright industries contributed $535 billion dollars to the U.S. economy – that's more than 5 percent of the gross domestic product. Weakening the DMCA would be tantamount to slamming the brakes on that growth. Without these protections, fewer companies and individuals will be willing to put their works into digital format. That would dramatically slow the creative genius that has fuelled the expansion of the Internet and e-commerce. Without the DMCA, Internet (and digital media) users could soon find themselves with nothing to use fairly.[1]

There is no question that debate over "DRM" and copy protection technologies among the technology and content industry groups and consumer fair use activists is spirited. However, at the end of the day, one must evaluate existing and proposed intellectual property protection and rights management solutions based on not only the effectiveness, security, flexibility, and implementation cost of the technologies, but also on their transparency and ease-of-use by consumers.

Legislative Intent of Fair Use and the DMCA

As stated earlier, fair use is not an absolute right, but, rather, a balance between the rights of consumers to use technology and the rights of creators to extract the economic value of their work, and a defense against alleged copyright violations. This balance was incorporated into the 1976 Copyright Act in section 106, which grants copyright holders certain enumerated rights, and section 107, which codifies the fair use doctrine. The courts have established case law precedence dealing with the fair use concept, and are perfectly capable of administering the law with respect to the DMCA.

Prior to codification, fair use was developed through common law as an equitable principle. Section 107 of the 1976 Copyright Act does not define the term, but lays out some general guidelines by which fair use may be ascertained, and provides some examples of what might be considered fair use, including criticism, comment, news, reportage, scholarship and research. According to both the House and Senate, section 107 is not intended to alter the scope of fair use or strictly define it, "The statement of the fair use doctrine in section 107 offers some guidance to users in determining when the principles of the doctrine apply . . . The courts must be free to adapt the doctrine to particular situations on a case-by-case basis." S. Rep. No. 473, at 62 (1975); H.R. Rep. No. 1476, at 66 (1975).

In the past few years, the copyright protection dynamic has change dramatically – from that of photocopies and illicit analog recordings to that of widespread electronic shoplifting. The Internet,

[1] Robert Holleyman "If content is pirated, eventually it vanishes." May 20, 2002 posted in The San Jose Mercury News.

and other digital technologies, enables the mass copying and distribution of all kinds of works. In 1998, Congress enacted the DMCA to bring copyright law "squarely into the digital age," as well as to implement two World Intellectual Property Organization ("WIPO") treaties. The treaties required signatory countries to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used" to protect copyrighted works from infringement.

Congressional support for the DMCA was unanimous, supported by numerous statements from Senators and Representatives contending that the bill preserved fair use in the digital environment.

Congress took great pains to ensure that the DMCA did not conflict with or inhibit fair use as laid out in section 107 of the 1976 Copyright Act. According to the legislative history, Congress stated that section 1201(c) "is intended to ensure that none of the provisions in section 1201 affect the existing legal regime established in the Copyright Act and case law interpreting that statute." H.R. Rep. No. 105-551, pt. 1, at 20 (1998). In fact, the DMCA explicitly states that fair use will not be affected. Section 1201(c)(1) provides that "nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." Along those same lines, Congress "determined that no change to section 107 was required because section 107, as written, is technologically neutral, and therefore, the fair use doctrine is fully applicable to the digital world as in the analog world." S. Rep. No. 105-190, at 23-24 (1998).

Fair Use Concerns

Macrovision is has a singular focus on delivering intellectual property protection and digital rights management solutions to content owners and software developers throughout the world. Demand for our core technologies is linked to a number of critical trends and growth drivers: namely, the increased availability of "smart" digital devices, expanding network connectivity, the growing threat of digital piracy and security vulnerabilities, and shifts in content consumption and software usage. Macrovision strongly endorses the original tenets of the DMCA. In response to this Notice of Inquiry, a large number of the proposals employ the concept of fair use as the premise for exempting virtually every form of digital content from the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. Macrovision is sensitive to the concerns expressed by others with regard to the fair use provisions of Copyright Law and the anti-circumvention provisions in Section 1201 of the DMCA. However, we would like to bring to the Librarian's attention that copy protection and DRM technologies can, in fact, support fair use and allow time-shifting (use purchased product at a later date), space-shifting (use purchased product or program in one or more playback devices), and exportability and interoperability. Fair use, therefore, needs to be assessed in terms of reasonable expections in view of the increasingly flexible distribution and new usage models that are now enabled by the DRM technologies.

Macrovision's History

Since 1985, Macrovision has pioneered copy protection and rights management solutions for video, pay-per-view, DVD, consumer and enterprise software, and music CDs. We have been working cooperatively with a number of industry groups, such as the Copy Protection Technical Working Group ("CPTWG"), the Broadcast Protection Discussion Group ("BPDG"), the DVD Copy Control Association ("DVD CCA") and the Video Watermarking Companies ("VWM"), to design solutions that address the intellectual property protection challenges posed in both digital and analog environments. The DMCA demonstrated that positive government legislation and enforcement actions could effectively balance the diverse interests of consumers, the consumer electronics and PC industry and the copyright (content) industry.

Macrovision has copy-protected over 3.5 billion VHS videocassettes and, in the last four years, over 1.5 billion DVDs. Our copy protection technology is embedded in virtually all DVD players and recorders, in addition to more than 100 million digital set-top-boxes and personal video recorders, including over 90% of those used in the UK, North America and Japan. We have copy-protected over 200 million CD ROMs containing PC games and over 60 million music CDs. These statistics, and our company's extensive copy protection customer base, which includes all the major Hollywood studios, hardware suppliers to the satellite and cable TV industry, the major PC games publishers and the optical media manufacturing infrastructure – have resulted from a sustained 15-year focus on developing effective copy protection and DRM technologies. DRM technologies comprise various software-based electronic and security solutions that are designed to enable copyright owners to license and market their copyrighted content across a variety of mediums – from physical goods such as CDs and DVDs, wired or wireless electronic transmissions, to the Internet. Copy protection is a critical element of most digital rights management technologies.

Problem – Unauthorized Copying and Redistribution Trend (from Analog to Digital Media to the Internet)

As we've noted, today's "digital shoplifters" can employ PCs in the privacy of their own home, where they are immune from arrest by police and enforcement agencies, to essentially become widespread distributors of pirated content. In the physical world, many retailers estimate that they lose about 2% of their revenues to shoplifters. In the digital world, the pilferage is far higher. National consumer surveys have revealed that between 10-20% of the population routinely engages in some type of unauthorized video copying – whether using CD burners, videocassette recorders, or file sharing services. The losses in the software and music businesses appear to be far higher[2]. Many surveys have confirmed that a high percentage of teenagers and college students utilize CD burners to copy music albums and also share music files over the Internet with peer-to-

[2] The International Data Corporation ("IDC") estimated that the worldwide unauthorized software access and usage represented a total of $78 billion loss to the software industry; the International Federation of the Phonographic Industry ("IFPI") estimated software piracy loss from electronic media in 2001 was in excess of $4.2 billion to the recording industry, this not including Internet piracy.

peer file sharing services like KaZaA, Limewire, Morpheus, and others. In the past month, 321 Studios, a new company, has attracted considerable attention – and a content owner lawsuit – with their new DVD copying software that is purported to allow consumers to make copies of DVD movies without actually circumventing industry-standard encryption technology.

With the rapidly increasing advance of mass consumer broadband access, the requirement for enhanced content protection and secure DRM solutions has become even more urgent, since owners of premium content will not employ this medium unless their property is protected. The issues surrounding digital content delivery have become more critical: How do we safeguard digital content delivery and access? How do we protect the rights of the content owners once the content has been accessed? How do we enable flexible usage or re-distribution models, such that content owners and their distribution and consumer channels can optimize the advantages offered by the digital age? Without a secure solution, content owners are unlikely to authorize the transmission of their premium content, thereby limiting growth of both the content and hardware industries in the digital marketplace.

Need for Effective DRM and Legal Infrastructure

The solution to these problems is an effective content protection and DRM infrastructure, and a legal structure that protects copyright holders as well as technologists and consumer electronic manufacturers. One of the most dubious phrases used in the current inter-industry debates is that of copying for "fair use" or non-commercial benefit. If someone makes a copy of a DVD or TV program and puts it on the Web, it may well have been done for non-commercial benefit. However, it is unlikely that a rights owner (and the related supply chain), who may lose tens of thousands of displaced sales as a result, will feel that they have not suffered a significant commercial loss and infringement on their copyright.[3] Fair Use can be misused for unauthorized access and unauthorized reproduction or redistribution of copyrighted content. No one intended for the application of fair use to enable consumers to make unlimited unauthorized copies of protected work or to electronically transfer a copy of original content to an unauthorized Internet file sharing service. In the digital world, this concept of fair use must be clarified in such a way to protect the intellectual property owner. Copy protection and DRM technologies are designed to be flexible, adaptable, and transparent in order to support such personal rights as time-shifting, space-shifting, back-up copies, and using content on multiple hardware platforms.

Many consumer rights activists have warned that copy protection and DRM technologies will impose an unfair cost burden or user interface penalty on all consumers, since hardware and

[3] Unauthorized peer-to-peer networks are becoming a critical threat to the content and information industries. In its September 2002 Congressional hearing on "Piracy On Peer-to-Peer Networks," the Recording Industry Association of America ("RIAA") estimated that more than 2.6 million files are copied every month. Another research firm, Viant of Boston, estimated in June 2001 that more than 300,000 to 350,000 pirated movies are downloaded from the Internet worldwide everyday.

content prices will carry an intellectual property protection surcharge, and the technology is intrusive or burdensome. DRM systems are designed to be transparent and to enable additional features, rather than to be a limiting technology. Fortunately, most DRM and copy protection technologies can be implemented at a cost of pennies for each software unit (CD, DVD, Pay-Per-View or Video-On-Demand program) and nickels and dimes for each hardware device. The actual cost of these technologies (including all royalties and implementation costs) is on the order of a small fraction of 1% of the retail prices. This means that the DRM and copy protection costs are well under 10 cents per disc or per program, and in the range of 25 – 50 cents per hardware device. This is considerably under the 1-2% hidden tax that we, as consumers, have historically paid for physical goods – due to the fact that retailers gross up their prices in order to recoup shoplifting losses.

Solution – DRM Enables New Business and Supports Reasonable Fair Use Expectations

Effective copy protection and DRM technologies actually expand new business opportunities. Many articles written about copyright reform legislation point out that the Hollywood studios were able to grow a substantial video business, despite predictions of the obliteration of the movie industry once the VCR-installed base became significant. Of course, we all know that the VCR actually stimulated the growth of a $16 billion prerecorded media business, and the DVD format has extended that in excess of $20 billion. One fact that is often overlooked in this growth story is that, early on, the studios had access to a fundamental rights management technology – electronic copy protection on videocassettes – that meant they were not at risk to wholesale, unauthorized copying. With the introduction of DVDs, a new encryption technology and a new version of Macrovision's copy protection technology helped provide the copy protection security that was required by the studios before they would release their valuable movies on the new optical disc format. Without the strong anti-circumvention provisions of the DMCA, this $20 billion industry would be in serious jeopardy.

Conclusion

The video, music and software industries need more secure and more versatile intellectual property safeguards. At Macrovision, we believe that unless there is implementation of broadly-adopted technology-based copy protection and DRM solutions, content holders will be reluctant to release premium digital content or software through the Internet, which is essential for stimulating broadband and the consumer electronics sales. We believe that the private sector should take the lead role, in conjunction with supportive government legislation such as the DMCA, in proposing and implementing essential copyright areas, as well as managing compliance and enforcement. We believe that the DMCA was a well-conceived and clearly drafted piece of legislation, and should be left as is, especially with regard to the anti-circumvention provisions. It should be upgraded to allow copyright owners to utilize peer-to-peer file sharing decoys and to include the new watermarking technologies.

This letter, along with the attached Appendix, has attempted to describe how technology for content protection and DRM can provide for and support consumer friendly, robust, secure, and cost-effective solutions that enable copyright owners to navigate the digital highway with confidence and optimize the new opportunities offered by the "Broadband Economy" while enabling new distribution models to address reasonable consumer usage expectations.

In closing, I would emphasize three important points for the Librarian and Copyright Office to consider:

(1) Copyright protection and DRM technologies are essential tools for the U.S. intellectual property and copyright industries – which are the largest and most innovative in the world. They must be nurtured and protected by copyright laws – and that includes outlawing any circumvention devices, techniques, or Internet hacks that might be promoted in the name of "fair use."

(2) Copy protection and DRM technologies are proven, cost effective, and unobtrusive to the consumer. The free market economy is doing a good job at sorting out which competing products will win in the marketplace. However, in certain situations, such as video watermarking, where it would be costly to force the hardware manufacturers to implement multiple solutions, industry standards make sense. In these situations, the government needs to recognize that consortiums of companies should be allowed to come together to offer a single solution under fair and non-discriminatory terms.

(3) If industry groups cannot resolve their differences in a timely fashion, the government should be ready, willing, and able to establish standards and, if necessary, select certain technology solutions to promote the adoption and deployment of copy protection and DRM technologies such that the distribution of digital content is more rapidly encouraged. We believe the time has come for the government to take action with regard to both the 'broadcast flag' and the watermarking solution to plug the analog hole.

Macrovision is focused on delivering intellectual property protection and digital rights management solutions to content owners and software developers throughout the world. Our core technologies are linked to a number of critical trends: increased availability of smart digital devices, expanding network connectivity, growing threat of software/content piracy and security vulnerabilities, and shifts in content consumption and software usage.

Sincerely yours,

MACROVISION CORPORATION

William A. Krepick
President/CEO
Tel 408.562.8420
Fax 408.567.1802
E-mail: bkrepick@macrovision.com

APPENDIX

Example 1 – Video Copyright Management and Controlled Access To Digital Video Content

In the video industry, Macrovision is working to establish an effective digital video copyright protection ecosystem that includes bilateral watermarking solutions that are implemented in both consumer hardware and digital video content. Watermarking has been proposed by the DVD CCA industry trade group as an effective deterrent to unauthorized digital recording, as well as one of the few technologies capable of plugging the "analog hole."[1] Macrovision, Digimarc, Hitachi, NEC, Philips, Pioneer and Sony have formed the Video Watermarking ("VWM") Companies to offer a best-of-breed solution for digital video applications. The combined engineering talent, intellectual property, product performance, marketing and support infrastructure of our seven companies is unparalleled. These companies are known as leading innovators in their respective markets. The VWM watermarking technology is designed to protect video content on DVDs, videocassettes, cable or satellite transmissions, and the Internet from unauthorized copying to recordable DVDs, DVHS, personal digital video recorders ("PVRs") and multimedia personal computers.

Video Copy Protection

Macrovision's video copy protection technologies are designed to enable rights owners and program providers to protect their videocassettes, Digital Video Discs ("DVDs"), digital Pay-Per-View ("PPV") and Video-On-Demand ("VOD") programs from unauthorized recording onto VCRs. The technology is incorporated in virtually all DVD players, PC/DVD-ROM drives, DVD-based gaming consoles, and PVRs and in nearly 90% of all digital set-top boxes to protect against unauthorized recording of video programming. Macrovision's copy protection technology degrades unauthorized copies on approximately 95 percent of all VCRs.

DVD Copy Protection

The DVD copy protection process is activated during DVD authoring, when certain copy protection trigger bits are set to "ON." When the disc is played back in a consumer's home, these trigger bits activate a Macrovision-enabled digital-to-analog converter chip inside the player. The chip then applies copy protection to the analog output of the DVD player. This allows for transparent viewing of the original program, but causes copies made on most VCRs to be substantially degraded. In no way does it interfere with the consumer's enjoyment of the program.

[1] The analog hole refers to the situation where digital content is converted to analog format for viewing or manipulation, and then converted back to digital format for transmission or storage, and in the conversion process, the copyright protection and/or DRM schema is lost or circumvented. Watermarking technology is the only technology that can be transparently embedded within video itself – for either analog or digital format. It is the only technology that can survive multiple transformations between analog and digital, and hence it is a critical and necessary component technology for providing a comprehensive and pervasive copy protection ecosystem for digital media. The analog hole is like death and taxes – it will always be present for as long as humans use their eyes to view video programs.

PPV/VOD Copy Protection

The increased availability of digital-quality movies and events on direct broadcast satellite and digital cable systems raises an important challenge for the PPV and VOD industry. Specifically, many consumers can now make commercial-quality copies of PPV/VOD movies by simply pressing of their VCR record button. These copies, when passed onto friends, neighbors, and co-workers, can displace both video store rentals and initial and repeat PPV/VOD purchases.[2]

To apply copy protection to a specific program, the direct broadcast satellite ("DBS") operator or cable system operator transmits a software command from the uplink center or headend to its subscriber's set-top decoders. An integrated circuit inside the decoder receives the command and adds the copy protection waveform to the analog video destined for the TV. The copy-protected signal is transparent on original program viewing, but causes copies made on the majority of VCRs to degrade to the extent that they no longer have entertainment value. Currently, 32 system operators have licensed or specified Macrovision's video copy protection technology; 15 of the 32 system operators have activated the copy protection. Set-top decoder manufacturers provide copy protection capability by incorporating copy protection-capable integrated circuits in their decoders. Macrovision's copy protection is included in nearly 90% of digital set-top and PVR/DVR decoders distributed throughout the world. The technology is poised to play a key role in the growth of the VOD industry as content owners and system operators accelerate their copy protection activation.

Macrovision's video copy protection technology has been utilized on over 3.5 billion VHS videocassettes, on over 1.5 billion DVD discs, in over 100 million digital set-top boxes and PVRs and 100 million DVD devices. The technology has been licensed to 343 DVD authoring facilities, 98 replicators, 237 duplicators, 271 DVD device manufacturers, 68 digital set-top box and 9 PVR manufacturers and 58 IC component suppliers, worldwide.

DRM for Video and Multimedia Content

Macrovision's DRM technologies are designed to combat widespread casual piracy while offering solutions that enable our customers to electronically control the use of digital content and software – which facilitates significant new revenue models.

Macrovision's MacroSafe™ DRM is a multi-layered software solution for the secure distribution and management of video, audio, graphics, and other multimedia applications for PCs, as well as for a variety of non-PC devices including set-top boxes, PDAs, portable entertainment devices,

[2] According to five U.S. surveys conducted by Alexander & Associates, Inc., in which it interviewed an average of 1004 TV/VCR homes using its Video Flash weekly Omnibus, an estimated 31.6 million PPV programs (or 26.6 million PPV movies) were copied over a 12-months period.

and digital consumer electronics appliances. It is a complete security solution for electronic delivery of high value content – its transparent architecture causes little or no impact to the existing content creation work flow, neither to the electronic delivery infrastructure, nor to the consumer's viewing experience. And because MacroSafe is based on industry standard, non-proprietary programming languages, interfaces and protocols, it can be quickly and cost-effectively integrated into embedded devices, consumer electronic set-tops, and into an existing e-commerce and delivery system. MacroSafe is currently in the market introduction and testing phase, and is expected to be deployed over the next 3 years.

Example 2 – Ability to play DVD movies on PCs in secure environment

Macrovision has integrated its latest MacroSafe™ with InterVideo's WinDVD, the world's most popular DVD player. The two companies will also join in co-marketing efforts to promote this secure solution to the video on demand market.

MacroSafe is a complete end-to-end digital rights management solution for the secure distribution and consumption of high value video, audio and other multimedia content to PCs, personal video recorders and set-top boxes.

InterVideo's WinDVD 4 is the most sophisticated DVD-playing software on the market and is bundled with 9 of the top 10 PC makers in the world including Dell, HP, Sony, IBM and others. In addition to playing DVDs, WinDVD can also play MPEG-1, MPEG-2 and DivX™ content from files, such as those that might be downloaded from an Internet movie rental site.

The integration of the MacroSafe client with the WinDVD player enables the combined solution to:

- Recognize content that has been encrypted and protected using the MacroSafe system
- Determine if the user has the right to view the content
- Enable easy playback of the content, if appropriate
- Inhibit unauthorized peer-to-peer file sharing

The integration of the two products is a benefit to the content owners, content distributors and the viewers of the content. Content owners can be confident that their high value media is delivered encrypted to the end viewer and is only decrypted per the granted usage models. Content distributors can be confident that a high quality, off-the-shelf solution is available for the playback of MacroSafe-protected content. And viewers of the content can be confident that they will have an experience similar to the one they have when viewing a DVD.

Example 3 – Music CD copy protection, authentication, and controlled burning solutions with DRM interoperability

The music industry has been without effective copy protection since the advent of the CD. The proliferation of inexpensive and easy-to-use CD-burners and CD-recordable media over the past 3 years, and the adoption of Internet peer-to-peer file sharing has dramatically impacted music industry and caused continuing 10% per year declines in revenues.[3] According to various industry reports, over 25% of the 5.2 billion CD-R blank media sold worldwide were used for audio compilations and home recording of music content.

Macrovision has developed effective copy protection and authentication solutions for music CDs that integrate with DRM systems to allow music labels to both protect their content and enable consumers to make limited copies and compilations of CD albums. A copy-protected and DRM-managed CD can allow this while actually enhancing the consumers' music experience. A new category of multi-session copy-protected and DRM-managed CDs will provide consumers with new features via computers and the Internet, thus providing additional entertainment features and added value that had not previously been made available on non-copy-protected, non-DRM-enabled CDs.

Our CDS-100 and CDS-200 copy protection technology has been used on approximately 60 million music CDs. Our CDS-300 technology for music CDs allows consumer device playability, PC playability, and allows the consumer to make a back-up copy on their PC for personal use – and enables the music to be played from the PC without the original CD present. Macrovision is working with Microsoft and other DRM providers to integrate optical disc authentication and controlled burning technologies to enable more consumer features.

We are working hard to introduce "controlled CD burning" capability in mid-2003, which will support reasonable consumer expectation of fair use – just as music fans took it as their right to make a back-up cassette copy of their vinyl album for their personal use, controlled burning functionality will enable consumers to make a back-up CD copy for personal use (or make 2 or more copies, whatever rights as may be granted by the rights owners based on new distribution models that the consumer may subscribe to) – while, at the same time, preventing the unlawful activities of digital pirates.

Transparent to the music label, the audio CD technology is easily implemented in the CD manufacturing process with no production machinery modification or changes to the pre-mastering process necessary. Transparent to the consumer, music CDs protected by the CDS-300 technology play on commercial CD players while preserving the original quality of the content.

[3] RIAA and IFPA reported a continued 10% decline in worldwide music CD sales for the past 2 years. If the current trend continues, the recording business may literally cease to exist.

Example 4 – Electronic License Management and Product Activation for Software

In the software industry, Macrovision has been at the forefront of providing copy protection solutions for both consumer and enterprise software. We are the world's leading provider of PC games' copy protection systems and our SafeDisc® technology is routinely used on 70-80% of all hit title PC games. Companies like Microsoft, Electronic Arts, Take2 Interactive, and Hasbro use our SafeDisc technology to prevent consumers from copying their game CDs. Other well known software companies such as Intuit, Apple, AutoDesk, and MathSoft, use our SafeCast® DRM solution to help them securely distribute their application software and ensure that consumers are in compliance with the license terms of use. Another 2,500 software companies have used our FLEX*lm*® electronic license management software to help them in a corporate environment ensure that the corporate end-users are in compliance with the terms of their licenses and that the actual number of users matches the number authorized in their respective contracts.

Consumer Software Copy Protection

With the increased availability and reduced cost of CD-R writers, copying has never been easier. The total estimated value of unauthorized copies of PC application software CD-ROMs among consumer households is estimated to approach $675 million in the U.S., according to two studies sponsored by Macrovision Corporation and conducted in 1999 and 2000 by San Mateo, CA-based Merrill Research & Associates. In 69% of the cases where unauthorized copies were made or borrowed, respondents indicated they would have purchased the software if copying were not an option.

The software industry's piracy studies only quantify losses due to piracy, more commonly referred to as packaged goods counterfeiting. Losses from casual copying quantified in the Merrill Research studies are additional losses to the industry. The first Merrill Research study was conducted in March 1999, which was the first to quantify that close to $830 million in PC entertainment software has been copied in the U.S. in the same year. The displaced retail sales loss of games and "edutainment" software was then estimated to be $480 million based on the respondents indicating that they would have purchased 58% of the games software if copying were not an option. The follow-on 2000 study further estimated that casual copying of *consumer software applications* might represent additional displaced software retail sales of nearly $470 million (i.e., 69% of the estimated $675 million unauthorized software application CD-ROMs in consumer households). These studies suggest that the software industry losses to piracy needs to be measured in two ways – packaged goods counterfeiting by "professional" pirates and unauthorized casual copying. The Business Software Association (BSA)/ Software Information Industry Association ("SIIA") reported an estimated $2.9 billion software revenue loss per year due to piracy in the U.S. alone, representing a 25% piracy rate (or one in every four applications) in the U.S., coupled with a market that represents over 43% of the business software in use globally. The above was based on piracy loss due to packaged goods counterfeiting to an estimated $11.2 billion worldwide number. Taken together with the Merrill Research casual

copying estimates, the combined $4.4 billion loss demonstrates a much higher (38%) piracy rate than previously assessed by the software industry. This would suggest that **'two in every five applications'** might be pirated or copied in the U.S. The Merrill study supports that the true piracy rate can be reduced by 20% with the use of copy protection technology effective against unauthorized casual copying at home and in the workplace.

PC-CD/DVD-ROM Copy Protection

Macrovision's patented SafeDisc® technology protects CD-ROMs from unauthorized replication or copying, thus encouraging users to purchase legitimate copies. It is easy to apply by the publisher and is completely transparent to the consumer. It is currently the most widely used copy protection solution for Windows® and Apple® Mac® platforms. With over 200 million software CDs manufactured using SafeDisc, Macrovision's copy protection solution has established itself as the *de facto* standard in CD-ROM copy protection.

SafeDisc is a software-based solution that does not require any changes to the publisher's application code and is compatible with standard PC or Mac environments and CD-ROM hardware. It is comprised of authenticating digital signatures embedded on the CD-ROM disc, an encryption wrapper, and an anti-hacking technology, which is added at the time of encrypting the application and secures the CD-ROM executable. The patented SafeDisc digital signatures are added to each original disc during the mastering and replication process, and prevent copying by standard CD-R drives. For additional protection, developers can also use the SafeDisc API. The SafeDisc API has been developed to work in conjunction with the wrapper security. The publisher can use the API so that it ties the protected application closely with the SafeDisc security system. SafeDisc is available at over 110 mastering and replication facilities worldwide.

DRM for Software Activation and Flexible Distribution

Macrovision's SafeCast® DRM and license management technology offers software publishers and developers the opportunity to broaden their market reach and boost sales by distributing and promoting their offerings in a variety of innovative ways. It is an exceptionally flexible and highly secure DRM system for software. It replaces expensive hardware "dongles" with reliable software-based security. With SafeCast protection, software publishers can deliver products via any physical media (CD or DVD) or electronic (Internet transmission) digital medium, and still retain complete control over how and when they can be "unlocked" and used.

Product Activation is a technology that allows software publishers to reduce and control unauthorized use of their products. By requiring each customer to activate his or her copy of a software product before using it, Product Activation can effectively prevent that product from being passed along to other users in violation of the license agreement. SafeCast Product Activation system actively prevents unauthorized use of software, by adding several layers of security:

- SafeCast "locks" the protected/encrypted software so that it cannot be used until it has been properly activated.
- The serial number entered by the user is checked against a central database. The product is only activated once the serial number has been validated, and SafeCast ensures that only activated software will correctly "unlock" (decrypt) itself each time it is run.
- SafeCast links the protected product to the computer on which it is installed, using a technology called "System Binding", to prevent the activated software from being copied and used on another computer.

These security measures can be implemented so as to be maximally convenient for legitimate users (and, in fact, almost completely transparent to the Internet connections) while, at the same time, effectively guarding against unauthorized use of the protected software.

In addition to Product Activation, SafeCast enables a wide range of secure eCommerce and Electronic Software Distribution solutions. Publishers/resellers can create trial and demo versions of software applications in minutes, without recompiling, and allows "Try & Buy" customers to purchase the products with a few clicks and a credit card. SafeCast enables software subscription and rental models, providing publishers/resellers with an ongoing revenue stream.

SafeCast secures executable programs, DLLs and COM objects, and protects multiple executables within a single product. The SafeCast Wizard makes it easy to add security and rights management to finished products, without changing the code or recompiling.

Expanding Electronic Licensing for Software Delivery

The software market is transitioning from physical packaged goods with tightly defined functionality to software delivered as a service. The availability of corporate bandwidth, always-on connectivity, the need to improve return on investment, and the desire to serve *all* potential individual users regardless of how casual their use pattern (or how little they are willing to pay) are factors leading software vendors to explore alternative methods of producing, valuing and selling software.

Macrovision's leading FLEX*lm*® product enables electronic licensing compliance for any kind of application software either on individual computers or within a network environment. It has become the *de facto* commercial electronic license management ("ELM") standard that has been licensed to over 2,500 software vendors worldwide. Macrovision has expanded the electronic licensing and license delivery "software service ecosystem" with FLEX*bill*™, a usage-based licensing technology that allows users to pay software vendors based upon authenticated usage reports generated at the user's site and automatically transmitted to the vendor. FLEX*bill* provides

an easy and effective way to manage and track license usage and enables a variety of pricing and licensing strategies, leading to higher revenues for vendors *and* higher customer satisfaction for users. Additionally, software vendors that deploy FLEX*bill* can obtain key business intelligence such as identifying which software components their customers value most, thus leading to informed strategic business decisions, increased customer retention, deeper market penetration.

FLEX*lm*® is a software application toolkit that electronically enforces the software vendors' licensing policies either on individual computers or within a network environment.[4] FLEX*lm* is available for MS® Windows®, Solaris, AIX and other UNIX variants, three Linux variants, and selected embedded operating systems, and supports over 100 different license types which, on a combined basis, enable thousands of unique business models. Its companion product, FLEX*bill*™, is a license management solution based upon FLEX*lm*, allow vendors to implement "Pay As You Go" pricing models through analysis of authenticated usage log files.

Electronic License Delivery ("ELD")

One of the most effective ways for software vendors to distribute and for software customers to receive electronic licenses is via the Internet. Vendors can achieve lower cost of operations and increased sales, while their customers can gain access to new licenses 24 hours a day, 7 days a week. Macrovision's GT*licensing*™ is a "back office" solution for the generation, management, tracking and delivery of FLEX*lm* electronic software licenses.

GT*licensing* is a complementary product to FLEX*lm*. It is a highly scalable, enterprise-class software solution that supports a wide range of digital licensing functions, including the automatic generation and distribution of licenses over the Internet, 24 hours a day, 7 days a week. It provides software vendors the capability to support a wide range of licensing schemes, manage all the information pertaining to customers and their licenses, and permits the distribution of license certificates by various means. In keeping with industry trends, GT*licensing* now uses technologies such as XML and JSP, making it easier for software vendors to integrate the product to better fit their licensing policies, and to modify customer license fulfilment web pages to provide a higher level of customer satisfaction. It is compatible with a host of the most popular network platforms and operating systems, including Windows, Solaris, and Linux.

Managing Unauthorized Digital Content in the Workplace

Unauthorized peer-to-peer networks are becoming a critical threat to the content and information industries. The Internet's growth and the associated expansion of high-bandwidth connections within workplaces has, unfortunately, exposed a lot of companies to employees knowingly or unknowingly swapping unauthorized music or video files, or downloading pirated software at

[4] According to International Data Corp.'s ("IDC") latest research on software piracy, for every licensed software application, there are estimated minimum of 5 un-licensed usages, representing a compounded loss of $78 billion revenues last year to the worldwide software industry.

work.[5] Corporations have been increasingly held liable for allowing illegal copyrighted materials in their workplaces.

In October 2002, Macrovision and Websense announced a strategic partnership to combat the growing problem of unauthorized digital content in the workplace. Both companies – leaders in their respective markets – will develop complementary solutions designed to prevent the unauthorized storage, use and distribution of copyrighted content within enterprise, government and educational institutions worldwide. These joint solutions will benefit content providers and employers by providing a proactive defense against legal liabilities associated with unauthorized games, music, video, software and other digital content on company computing resources.

The solutions will combine Macrovision's proprietary technologies and long-standing expertise in the field of digital signatures and fingerprints and Websense's patent-pending content classification technologies to identify and control the downloading of hacked content and unauthorized redistribution of copyrighted material.

The first product from the partnership is expected to be launched by Websense in the second half of 2003. The product, a Liability Protector add-on module for Websense Enterprise software, would help shield employers from potential legal liabilities by searching company servers and hard drives for copyrighted content found to have copy protection elements removed or bypassed from Macrovision's patented technologies for video, audio and software applications. Coinciding with the release of the Websense Liability Protector module, Macrovision intends to launch SafeScan™, a product allowing Macrovision's current CD-ROM copy protection customers to extend the copy protection ecosystem for those games that have been protected with Macrovision's patented SafeDisc® technology. SafeScan is designed to prevent downloading and file sharing of hacked content in workplaces.

The concept of content security has broadened from a point focus of isolating security breaches in one distribution venue to a broader solution to limit the damage from any potential breach across venues. SafeScan is an important step in expanding our content protection offerings into the enterprise space to encompass public and private networks, and to monitor and control copyright abuse such as unauthorized peer-to-peer file sharing.

[5] A high percentage of unauthorized content is downloaded at work due to the broad availability of bandwidth and the ability to execute otherwise time-consuming downloads. In fact, according to recent report from Jupiter Media Metrix, only 16 percent of home users have high-speed Internet access. By contrast, 57 percent of employees at work with Internet access use a broadband connection. By 2005, Jupiter predicts that number to increase to 87 percent of all employees.