GLENN D. POMERANTZ (SBN 112503)
*Glenn.Pomerantz@mto.com*
BART H. WILLIAMS (SBN 134009)
*Bart.Williams@mto.com*
KELLY M. KLAUS (SBN 161091)
*Kelly.Klaus@mto.com*
MUNGER, TOLLES & OLSON LLP
355 South Grand Avenue, Thirty-Fifth Floor
Los Angeles, CA 90071-1560
Tel: (213) 683-9100; Fax: (213) 687-3702

ROBERT H. ROTSTEIN (SBN 72452)
*rxr@msk.com*
ERIC J. GERMAN (SBN 224557)
*ejg@msk.com*
BETSY A. ZEDEK (SBN 241653)
*baz@msk.com*
MITCHELL SILBERBERG & KNUPP LLP
11377 West Olympic Boulevard
Los Angeles, California 90064-1683
Tel: (310) 312-2000; Fax: (310) 312-3100

GREGORY P. GOECKNER (SBN 103693)
gregory_goeckner@mpaa.org
DANIEL E. ROBBINS (SBN 156934)
dan_robbins@mpaa.org
15301 Ventura Boulevard, Building E
Sherman Oaks, California 91403-3102
Tel: (818) 995-6600; Fax: (818) 285-4403

Attorneys for Plaintiffs



UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

UNIVERSAL CITY STUDIOS PRODUCTIONS LLLP, UNIVERSAL CITY STUDIOS LLLP, PARAMOUNT PICTURES CORPORATION, TWENTIETH CENTURY FOX FILM CORPORATION, SONY PICTURES TELEVISION INC., COLUMBIA PICTURES INDUSTRIES, INC., SONY PICTURES ENTERTAINMENT INC., DISNEY ENTERPRISES, INC., WALT DISNEY PICTURES and WARNER BROS. ENTERTAINMENT INC.,

Plaintiffs,

CASE NO. CV08-06412 SJO AJWx

**DECLARATION OF DR. JOHN P. J. KELLY IN SUPPORT OF *EX PARTE* APPLICATION OF PLAINTIFFS FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION THEREOF**

vs.

REALNETWORKS, INC.; and REALNETWORKS HOME ENTERTAINMENT, INC.,

Defendants.

I, John P. J. Kelly, declare as follows:

1. I am the President and CEO of the Kelly Technology Group, a technology research and intellectual property consulting firm. I hold Bachelor of Arts and Master of Arts degrees with Honors in Mathematics from the University of Cambridge, England, and a Ph.D. in Computer Science from U.C.L.A. From 1982 through 1986, I was a professor in the Computer Science Department at U.C.L.A. From 1986 through 1997, I was a professor in the Electrical and Computer Engineering Department of the University of California, Santa Barbara. I teach and consult in many different aspects of computer science and engineering, including computer hardware and software architecture and design, software engineering and fault tolerance. My particular areas of expertise include computer architecture, software engineering and "clean-room" development and evaluation, reverse engineering, operating systems (including real-time and embedded), network computing (including Internet computing), storage systems, fault tolerance, parallel and distributed computing systems, transaction processing systems, database systems, and program management.

2. As a result of my education and professional experience, I have extensive knowledge of data security on peripheral devices such as CD-ROM and DVD drives, and magnetic-strip and bar-code readers, as well as in encryption and coding theory for information transfer — including, for example, network traffic between computers and bus traffic within computers. I also have experience with data security in financial transaction management systems.

3. As a result of my education and professional experience, I have extensive knowledge of computer software. Much of my research, including my Ph.D. dissertation and other publications, has concerned computer software, as has much of my professional consulting practice. I have worked in the area of software design and development for over thirty years. I have extensive experience in the design and development of small and large scale software systems. I have been involved

in the specification, development, integration and testing of computer systems with a wide range of requirements, sizes and types. I have designed, developed and analyzed source code on various development platforms including Windows, Linux, Unix, AS/400, AIX, and Sun Solaris, among others, and in a variety of programming languages including C, C++, C#, Java, Visual Basic, assembly language, and many others.

4. As a result of my education and professional experience, I have extensive knowledge of computer networking, hardware, software and databases. For example, from 1978 to 1995, I specified, designed and implemented distributed database architectures, systems and applications for Los Alamos National Laboratory and NASA's Jet Propulsion Laboratory. From 1985 to 1998, I consulted for AT&T GIS, NCR, Symbios Logic, and LSI Logic, including working as a member of the AT&T GIS Science Advisory Committee ("SAC"). The SAC evaluated AT&T's organization, technical direction and product strategy and made recommendations to the Vice President of Technology and Development.

5. I have knowledge and understanding of the technological components of the DVD Content Scramble System ("CSS"), based on prior work studying the hardware logic of DVD drives and the computer hardware and software that interacts with DVD drives. I make this declaration in support of Plaintiffs' application for a temporary restraining order and order to show cause. Below I describe the operations of Defendants' RealDVD software. I have personal knowledge of the following facts and, if called and sworn as a witness, could and would competently testify thereto.

## TECHNOLOGICAL PROTECTIONS PROVIDED BY CSS

6. The "DVD players" I am discussing in this declaration are software programs which will play a DVD on a computer screen or to a television connected to the computer.

7. The "DVD drives" I am discussing in this declaration are the physical hardware connected to a computer, into which DVDs are inserted and which read and output data off of a rotating DVD disc.

8. "CSS" or the "Content Scramble System" is a data encryption and authentication scheme intended to prevent copying video files directly from a DVD disc.

9. A DVD which contains a motion picture protected by CSS has three main components.

a. The first component is a recorded data area which includes encrypted "video object" files (.vob files) and related files (.ifo and .bup files) organized in sets called "title sets" in a file directory. The .vob files contain still images, video streams, audio streams, subtitle streams and menus; thus, one .vob file may correspond to the main menu of a DVD, another to part of the film, and another to a director's interview or other "special feature" included on the DVD. On CSS-encrypted DVDs, the .vob files are encrypted — with each "title set" encrypted differently, according to an individual "title key." Ultimately, these files must be decrypted to be played by a DVD player. The .ifo files contain information about the content stored in corresponding .vob files, and how that content can be accessed directly. The .bup file is a backup of the .ifo file. Both the .ifo and .bup files are composed of binary data.

b. The second component is a secure "lead-in" area of 2048 bytes. Physically located around the inner edge of the DVD, the "lead-in" area does not contain video data but contains a secret key — called the "disc key" or "content key" — necessary for decrypting the encrypted .vob files on the disc. The content key for the movie is itself encrypted, with the keys necessary to decrypt the content key provided to legitimate DVD players by

the DVD CCA (these keys are called "player keys"). Thus, a given DVD is protected by multiple layers of encryption.

c. Finally, the third component is a "lead-out" area, physically located around approximately the outermost millimeter band of the DVD, which signals to a DVD player when it reaches the end of the recorded data area of the disc.

10. "Encryption" in this context, refers to a method of scrambling data using complex mathematical formulas, or algorithms. The algorithm is given both the data to be protected and an encryption key — a long, variable number, used with the algorithm to encrypt the data. The data can then be accessed only by using a second "reverse" algorithm along with an appropriate decryption key.

11. In addition to multiple layers of encryption, CSS includes a further technological measure: an authentication scheme. Authentication is a well-recognized technique to preserve the security of computer information. It is a way to ensure the legitimacy of an entity seeking information. As an example, the password schemes used on many personal computer or email systems is a simple form of authentication.

12. The authentication that takes place between a DVD drive and a DVD player is significantly more complex than a password, and allows — through several "handshakes" and transfer of different codes — the drive to verify that the player is legitimate. When a CSS-protected DVD is inserted into a drive, that drive will not read or output data from that disc until an authentication process takes place between the drive and the player. In effect, the DVD drive automatically "locks" when a CSS-protected disc is inserted into the drive. A DVD drive must receive appropriate secure "keys" from a DVD player before it will permit access to the information encoded on the CSS-encrypted disc — in effect "unlocking."

13. The multi-step authentication process works as follows:

a. The DVD player initiates the process by sending a request to the DVD drive. In response, the Drive sends over a "grant ID."

b. Once it receives the "grant ID," the DVD player generates a response to the drive and sends its "player key" — assigned to it by the DVD CCA. With this response and this key, the drive verifies the player.

c. After this has occurred, the drive sends back a new key — generated by combining the DVD disc's "content key" obtained by the drive from the lead-in area with the player's "player key" — to the DVD player.

d. Thereafter, the DVD player sends a request to the DVD drive to send a "challenge key"; if the drive responds with a correct "challenge key," the DVD player can verify that the drive is legitimate.

e. Finally, the DVD drive and DVD player will negotiate a "bus key," which they use to encode their communications during the playing of the particular DVD in the drive. Such a "bus key" is used to obfuscate the communications between the drive and the player. This provides yet another layer of protection against unauthorized interception of communications between the drive and the player.

f. Only after this entire process has occurred will the DVD drive set the "authentication success flag," thus permitting the DVD player to access encrypted sections of the DVD.

14. But even after this authentication process has occurred, and thus the DVD drive is effectively "unlocked," the DVD drive will not permit an unauthorized program from reading or accessing information in the lead-in area of the disc where the "content key" is stored. For example, even after a DVD drive has completed the authentication process, the user cannot use a file browser to access or copy the lead-in area.

15. The end result of all of these layers of protection is that a consumer cannot make playable copies of a CSS-protected DVD.

## REALDVD MAKES PLAYABLE COPIES OF CSS-PROTECTED DVDS

16. On or about September 18, 2008, my staff and I obtained a laptop on which a purchased copy of RealDVD had been installed. The software had a version number of 1.0 and a build number of 1.0.0.493. The laptop also included a small installer file, left over from the installation process, which — when we ran it — downloaded the rest of an executable installation program. With this program, we were able to download 30-day trial versions of RealDVD software from Real's web site onto two additional computers; these copies of the software were also version 1.0, but had build numbers of 1.0.0.496. There were no visible differences between the three copies of the software.

17. Using these three computers, containing three copies of RealDVD software, we were able to make playable, persistent copies of several movies from CSS-protected DVDs, including "My Cousin Vinny," "Batman Begins," and "City of God."

18. When a user inserts a CSS-protected disc into her personal computer and starts up the RealDVD program, RealDVD will immediately display a menu displaying the title of the DVD and presenting the user with three options: "Play," "Save," and "Play and Save." As soon as the user picks one of these options, the DVD will begin spinning in the drive and RealDVD will complete the authentication process with the drive; thereafter, the drive will release the encrypted contents of the DVD.

19. If a user chooses either "Save" or "Play and Save," RealDVD will immediately begin copying the disc. On the computers we used, saving a movie took from approximately thirty minutes to two-and-a-half hours, depending upon the amount of memory, the processor, and other aspects of the computer used.

20. RealDVD allows a user to save a DVD to the internal hard disk of a computer or to any portable hard drive (*e.g.*, connected by USB or IEEE 1394 Firewire protocols).

21. In the process of saving a CSS-protected DVD, RealDVD creates a folder with the title of the movie (*e.g.*, "Cousin Vinny"). Inside the folder is a subfolder entitled "VIDEO_TS" as well as two files: (1) rdvdmovieinfo.xml and (2) video_ts.edf. The former file, rdvdmovieinfo.xml, is an unencrypted plaintext file which contains information about the copied DVD. The latter, video_ts.edf is an encrypted binary file; I discuss the likely contents of that file, below. (In some cases, RealDVD will also create a subfolder called "AUDIO_TS.")

22. The overall size of all of these files created by RealDVD varies by movie. The total size of all the files created by RealDVD for the copy of "Batman Begins" was 7.17 GB; for "City of God," 7.5 GB; and for "My Cousin Vinny," 6.9 GB.

23. In the subfolder "VIDEO_TS" is a file hierarchy identical to that on the original, physical DVD. Within the folder are the identical number of .vob, .ifo and .bup files as appeared on the original DVD; the file-size of each of these files is also identical to that on the original DVD. The contents of the files displayed, however, have been modified and thus are different; it is possible that this is as a result of RealDVD's having encrypted those files.

24. The overall contents of the "VIDEO_TS" subfolder are identical in size, location, and number to the file directory of the original DVD.

25. After RealDVD has completed copying a DVD — thus creating the above-mentioned file system — it ejects the physical DVD. A user of RealDVD can thereafter play back the copied DVD directly from her hard-drive, without the DVD being present in the drive. The copy played by RealDVD from the hard drive has no discernible differences from the original video played from the DVD, and includes all menus and special features. Thus, it is clear that RealDVD has made a copy of the data contents of the protected DVD.

**BY COPYING THE CONTENT KEY TO A USER'S HARD DRIVE, REALDVD BYPASSES TECHNOLOGICAL MEASURES DESIGNED TO PREVENT THE MAKING OF PLAYABLE COPIES OF DVDS**

26. As described herein, RealDVD makes a copy of the entire file-system of a DVD to the hard-drive of a user.

27. According to official RealDVD publications, the program does not decrypt those files before saving them; thus, they remain encrypted with CSS. Attached hereto, as Exhibit A, is a true and correct copy of a RealDVD press release indicating that the program "saves a secure copy of a DVD to the hard drive without removing or altering the CSS encryption."

28. In such encrypted state, the files are not immediately playable. In order to play back those copied files, they must first be decrypted. Thus, RealDVD must be decrypting those files upon playback. The only way to accomplish such decryption is for RealDVD to have access to the necessary "content key," usually located in the lead-in area of a DVD.

29. As described above, RealDVD plays copied DVD movies even if no DVD is present in the DVD drive. If no DVD is present during such playback, then RealDVD must have copied and stored the necessary content key; there is no other way to maintain CSS encryption of the files and yet be able to play them for a user after the physical DVD has been taken out of the drive. Thus, RealDVD copies and stores the content key on a user's hard drive. By doing so, RealDVD bypasses a technological measure designed to prevent the making of playable copies of DVDs.

30. When a movie is copied, a file named video_ts.edf is created by RealDVD in the movie's dedicated folder; this file may be where the content key has been copied to the hard drive. The video_ts.edf file is an encrypted binary file. The size of this file, for the movies we tested, was exactly 2400 bytes — just slightly larger than the size of the lead-in area on a CSS-encrypted DVD, which is 2048 bytes. RealDVD cannot play back a copied movie if the video_ts.edf file is

absent. Furthermore, the video_ts.edf does not appear to correspond to any file on the physical DVD.

## REALDVD BYPASSES CSS AUTHENTICATION

31. A DVD copied to a user's hard drive by RealDVD will play back normally from the hard drive even if no DVD drive is connected to the computer; thus, the DVD drive is not required for RealDVD to play back the CSS-protected video. As a result of this lack of interaction, RealDVD bypasses the authentication process that usually takes place between a DVD player and drive before a user can play a DVD.

32. As described above, a user wishing to watch a DVD movie usually begins by putting a disc in the DVD drive which, recognizing that the disc is protected, will "lock" — that is, refuse to read or output data until it has gone through a process of authentication with the player. Authentication requires that both the DVD player and drive transmit multiple "keys" to one another, verifying that each is authorized, as well as develop a "bus key" to obfuscate their communications, before a DVD dive will permit access to the encrypted sections of a protected DVD. This process ensures that only authorized players can have access to the encrypted contents of a DVD.

33. RealDVD, before it plays a CSS-protected copy of a DVD, does not engage in authentication with the drive. The drive is not involved in the process at all but, rather, has been entirely bypassed. RealDVD, instead, proceeds directly to playing the CSS-encrypted content of a copied DVD. By thus permitting playback of CSS-encrypted video without using the drive, RealDVD bypasses the technological protections against unauthorized access provided by the authentication process.

## REAL DVD BYPASSES CSS TECHNOLOGICAL RESTRICTIONS

34. Based on my above observations and my knowledge of the CSS protection system, it appears that RealDVD bypasses several important security protections embodied in CSS encryption and the CSS authentication system:

a. RealDVD provides users seeking to make copies of CSS-protected DVDs with access to the encrypted sectors of those DVDs by engaging in authentication with a DVD drive, and transmitting the necessary keys which establish that it is a safe, legitimate device. RealDVD then uses that access to permit copying of the copy-protected content of DVDs, thus impairing an important technological measure against copying.

b. RealDVD bypasses technological restrictions designed to prevent the copying of content in the lead-in area of DVDs in order to copy the "content key," which is specifically designed so as not to be subject to unauthorized copying. In so doing, it permits users to make *playable* copies of protected DVDs.

c. RealDVD, by allowing playback of a protected video without any interaction with the DVD drive, bypasses the CSS authentication process designed to prohibit unauthorized access.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct and that this declaration was executed this 30th day of September 2008 at Santa Barbara, California.

Dr. John P. J. Kelly

# 2008 PRESS RELEASES

Company
Press Room
Press Releases
2007
2006
2005
2004

## REALNETWORKS INTRODUCES REALDVD: THE BEST WAY TO WATCH DVDS

RealDVD Lets Consumers Save, Organize and Watch DVDs On Their PC and On The Go

**SAN DIEGO, CA, DEMOFall — September 8, 2008** — Digital entertainment services company RealNetworks® today unveiled RealDVD™, the first mainstream PC application allowing consumers to easily save their DVDs to their hard drive. RealDVD makes it easy to save DVDs to a PC or portable hard drive and watch them later without the physical discs. Unlike existing consumer applications on the market today, RealDVD is licensed DVD software that saves a secure copy of a DVD to the hard drive without removing or altering the CSS encryption.

"RealDVD gives consumers a great new way to get more out of their DVDs," said Rob Glaser, chairman and CEO of RealNetworks. "RealDVD continues in Real's tradition of consumer innovation over the past 15 years alongside RealAudio, RealJukebox, RealArcade, Rhapsody, and, most recently, RealPlayer 11."

RealDVD eliminates the hassle of searching through piles of DVD cases to find a missing disc and the disappointment of finding a favorite disc scratched and unplayable. Saving DVDs lets consumers create a valuable back-up copy of their digital library on their computer or portable drive for playback at home or on the road. RealDVD is ideal for traveling on business or entertaining the kids on a long trip with instant access to a variety of content and no physical discs to manage. Laptop users will appreciate improved battery life as the disc drive is no longer needed for video playback. Saving DVDs to portable hard drives creates an easy to manage personal library that is great for travel. Content saved to portable drives can be played on up to five machines licensed to an individual user.

**Fast Facts:**

- RealDVD saves an exact copy of the DVD image to a PC's internal or portable hard drive. Users can simultaneously watch and save a DVD
- Saved DVDs are then encrypted and locked again to make sure they cannot be shared or stolen
- Saving DVDs takes an average of 10-40 minutes, and takes up roughly 4-8 gigs of space
- RealDVD lets users pause and auto resume playback where they left off
- DVDs saved on a portable hard drive can be played on up to 5 PCs per user with an authorized copy of RealDVD
- Watching a saved DVD uses less battery life than viewing content from a disc in the drive
- Browse cover art, genre, title rating and actor information, imported automatically during saving
- Parental controls ensure children only access entertainment that is appropriate for their age

**Exhibit A, Page 11**

- Fifty percent of U.S. broadband households have over 50 DVDs in their collections, and last year consumers spent more than $16 billion purchasing DVDs *(According to TDG Reports & Screen Digest)*
- Hollywood shipped 1.1 billion DVD discs in 2007 — nearly 30 million more than in 2006 *(According to Screen Digest)*

In 1995 RealNetworks gave the Internet a voice with the first-ever Internet broadcast via the release of the RealAudio® Player, an innovation that garnered Real a coveted Emmy Award® by The National Academy of Television Arts & Sciences. Two years later RealNetworks became the first to bring streaming video to the Web with RealPlayer®, and followed that innovation with RealJukebox®, one of the first products allowing consumers to save their CDs to PCs, build media libraries and transfer to devices. Last year Real re-introduced a new version of RealPlayer, featuring a consumer-friendly download button that made it one-click simple to save Web video. RealDVD is the next step in bringing video entertainment to the PC.

RealDVD will be available this month from www.realdvd.com. Consumers can register to be one of the first to receive RealDVD for a limited-time discount offer of $29.99 ($20.00 off the retail price of $49.99). Additional licenses [up to 4] are available at a discounted price of $19.99.

**ABOUT REALNETWORKS**

RealNetworks, Inc. delivers digital entertainment services to consumers via PC, portable music player, home entertainment system or mobile phone. Real created the streaming media category in 1995 and has continued to lead the market with pioneering products and services, including: RealPlayer®, the first mainstream media player to enable one-click downloading and recording of Internet video; the award-winning Rhapsody® digital music service, which delivers more than 1 billion songs per year; RealArcade®, one of the largest casual games destinations on the Web; and a variety of mobile entertainment services, such as ringback tones, offered to consumers through leading wireless carriers around the world. RealNetworks' corporate information is located at www.realnetworks.com/company.



**Exhibit A, Page 12**