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. ALAN E. BELL 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.

DECLARATION OF DR. ALAN E. BELL

I, Dr. Alan E. Bell, hereby declare as follows:

1. I am Executive Vice President and Chief Technology Officer for Paramount Pictures, one of the Plaintiffs in this action. In that capacity, I am responsible for leading the company's efforts and strategy in connection with technology across a broad range of business areas centered on the preparation, distribution and consumption of digital motion picture content and related derivatives. My current areas of interest include the development of next generation digital distribution methods and emerging applications for internet-based communities, high definition disc formats, digital home entertainment networks, stereoscopic display and the technologies and issues associated with digital content rights management.

2. Before joining Paramount Pictures, I was Executive Vice President, Technology at Warner Bros. Technical Operations. I was centrally involved in the unification of the DVD format. Additionally, I am one of the founding co-chairs of the multi-industry Copy Protection Technical Working Group, which developed the CSS copy protection system (described below).

3. In recognition of my contributions to the DVD format and to original research in optical storage technology, I am an elected Fellow of the both the IEEE, the world's leading professional association for the advancement of technology, and the Optical Society of America. I received my doctoral and bachelor degrees in physics from London University. I make this declaration in support of Plaintiffs' application for a temporary restraining order and order to show cause. I have personal knowledge of the following facts and, if called and sworn as a witness, could and would competently testify thereto.

DVD TECHNOLOGY

4. The term "DVD" describes a high-capacity optical, digital storage medium, as well as a family of "standards" that describe how to store and read content on DVD discs.

5. In its most common deployment for motion pictures, a DVD will hold approximately nine gigabytes (9GB) of data.

6. Because of their storage capacity, DVDs are able to store the digital content that comprises a full-length motion picture. Subject to the security and encryption restrictions discussed below, DVDs are viewable either on a television equipped with a standalone DVD player or on a computer with a DVD drive and specialized playback software, known as DVD player software. DVDs have become very popular for the private home viewing of recorded motion pictures.

7. Motion pictures and other video content placed on DVDs are stored in a digital format. Unlike with analog formats, such as a VCR tape, the quality of content that is copied in a digital format does not generally degrade. Absent some form of encryption or other protection, digital DVD content is vulnerable to unauthorized copying.

THE DEVELOPMENT OF CSS

8. The DVD format was first completed in early 1995 but, because of concerns about unauthorized reproduction, each individual motion picture studio was unwilling to release films in digital format before an access-control and copy-protection system was available that would protect the digital movie content against unauthorized copying and distribution. To that end, the Copy Protection Technical Working Group (CPTWG) was formed, and the companies participated in meetings held from 1995 until November 1996. Representatives of the consumer electronics and information technology industries also participated in these meetings — which grew to include more than 120 people — with the goal of finding a content-protection system that provided effective protection for content-owners' works, was

reasonably feasible to implement in both computers and consumer electronics, and could be adopted as a standard across all three industries.

9. Matsushita Electric Industrial Co. Ltd. and Toshiba Corporation ultimately developed a system of authentication, encryption, and other technological restrictions, which became known as "CSS" (which stands for "Content Scrambling System"). The CSS copy protection system was adopted as the standard for video protection on DVDs and has been widely adopted by manufacturers of consumer electronics and computer devices. Since its launch, CSS has been used to protect billions of DVDs worldwide.

10. CSS technology — including associated intellectual property and technical specifications — is licensed to hardware and software manufacturers by an organization known as the DVD Copy Control Association ("DVDCCA"). DVDCCA evolved out of the Copy Protection Technical Working Group which developed CSS, and now DVDCCA controls all licensing of CSS technology and issues licenses to manufacture CSS-compliant devices. CSS has been licensed to hundreds of DVD player manufacturers (both hardware and software) and DVD content distributors in the United States and around the world.

THE PURPOSES AND OPERATION OF CSS

11. The purpose of the CSS copy protection system is to protect the contents of a DVD both from unauthorized access and from consumer copying. The mechanics of CSS differ slightly depending on whether the playback environment is a stand-alone DVD player or a personal computer. Because RealDVD operates in the personal computer environment, I will limit my discussion to CSS as it operates in the personal computer environment.

12. In the personal computer environment, DVDs are viewed using software players, like Windows Media Player. Manufacturers of software DVD players register with the DVD CCA in categories that correspond to the various parts of the CSS copy protection system that a software player has to interact with.

13. To protect DVD content, CSS relies on an integrated system of access "locks," encryption technology, and hardware and software restrictions. These restrictions provide multiple levels of protection against unauthorized consumer access and copying:

a. First, CSS provides for a "locking" mechanism whereby a computer's DVD drive will not allow access to the CSS-protected content on a DVD disc unless and until the DVD drive successfully engages in an "authentication" process confirming that the requesting program (i.e., player) is a compliant player and will properly protect the DVD digital content as it accesses and decrypts that content for the purpose of playback. If the requesting software cannot successfully authenticate itself (using a secret manufacturer's identification and algorithm licensed exclusively by the DVDCCA), the contents of the DVD will not be released by the drive or be transmitted to the computer for processing by the software program. This means that the software program will not be able to "read" the CSS-protected data — whether for purposes of playing the DVD, copying it, or otherwise.

b. Second, CSS uses encryption technology to selectively encrypt or "scramble" a substantial portion of the digital data that makes up each frame of a DVD video stream. The encryption of the DVD data is a level of security above and beyond the access control described above.

c. Third, even if a drive can be tricked into unlocking and transferring the encrypted digital contents, the presence of the CSS encryption prevents successful playback of the movie content. Successful playback of the CSS encrypted content requires that the content first be decrypted. Authorized decryption or "descrambling" requires multiple levels of "keys". To decrypt a CSS-encrypted DVD, a DVDCCA-licensed player must ultimately obtain the "content key." On CSS-encrypted DVDs, the content key information is itself protected by encryption and then located within a secure area of the

DVD called the "lead-in area." DVD drives do not permit any software other than a licensed DVDCCA player that can successfully complete the authentication process to have access to data in the "lead-in area." Thus, even if a software program might somehow succeed in reading and copying all of the encrypted video files off of a DVD to a hard-drive, that software program could not read or copy the "content key" necessary to decrypt those files. The resulting copy of the encrypted movie data thus could not later be successfully decrypted and played.

d. Fourth, the content key is *itself* encrypted or scrambled. To use the content key to decrypt the movie, a special "player manufacturer key" is required that is made available only to legitimate players by the DVDCCA. An authorized player will store its secret player manufacturer's key somewhere within its own software code, in a manner that hides or obfuscates the value of the secret key and prevents its being easily discovered.

e. Fifth, DVD drives capable of writing to blank recordable DVDs are not capable of writing to the "lead-in" area of a writable DVD. And commercially-available blank DVDs are specifically designed such that the "lead-in" area is not recordable. Thus, unless this protection is somehow defeated, it is impossible for a consumer to duplicate a CSS-encrypted DVD onto a new recordable DVD; that DVD will lack the necessary "content key" and other information contained in the "lead-in" area, and thus the CSS-protected movie cannot be decrypted or played. This technology, again, provides a further level of protection against unauthorized copying.

f. Sixth, content-owners can indicate directly on their DVDs that no copies are permitted to be made, using a standardized code called CGMS-D ("Copy Generation Management System – Digital"). This standard is incorporated into the CSS copy protection specifications. Under this standard, a movie studio can signal on a DVD that it is to never be copied, by assigning a value of "1,1" to two bits of data in a particular location as specified by the DVD format. All DVDCCA compliant consumer electronic DVD players and DVD software players for computers must comply with CGMS-D signals, and upon reading a signal of "1,1" are instructed to "CopyNever," and thus permit no copies to be made of the content.

g. Finally, in order to coordinate all of the above protection mechanisms, the DVDCCA grants licensees only limited authorization to use the "player keys" and specifications necessary to decrypt CSS. Each participant in the CSS system — disc manufacturers, studios, manufacturers of DVD drives, developers of DVD player software, etc. — gets only the information, including the confidential and the highly confidential information, it needs to accomplish its part of the system. Furthermore, the DVDCCA license does not grant licensed DVD players authority to permit the making of permanent, viewable copies of DVD content by accessing the encrypted video files and the "content key" from a CSS-encoded DVD. To the contrary, the license spells out in great detail numerous precautions to prevent copying, such as prohibiting unprotected (e.g., digital content that is not protected by encryption) digital "output" to a television that could be captured and copied. In addition the DVDCCA requires that CSS technology be maintained as confidential or highly confidential. These controls are intended to enhance the security of CSS and ensure that DVD player technology is used only to enable viewing — and not copying — of DVDs.

DEFENDANTS' REALDVD DVD-COPYING SOFTWARE

14. "RealDVD" is a software program that allows for the making of permanent, playable copies of CSS-protected DVD content onto a personal computer or portable hard-drive. I have personal knowledge of the operation of

RealDVD from having purchased and downloaded the software onto my personal computer, and having used the software on multiple occasions to copy DVDs.

15. RealDVD was briefly available online for download during the first days of September, 2008. I downloaded a copy during that time period.

16. Through operation of the RealDVD software itself, I observed that it permits users to "Play," "Save," or "Play and Save" a DVD inserted into the disc drive of a personal computer. If the user chooses either of the latter two options, RealDVD will make a copy of the entire contents of a DVD onto the PC hard drive. After the "save" operation is complete, the DVD drive ejects the disc, which may then be removed. I further observed that even after the DVD disc is removed from the drive, the RealDVD software allows me to playback the saved copy. The playback of the saved copy appears identical in all respects including menus, settings, and picture quality as if playback were being made directly from the disc that was previously present in the drive during the "save" process. Since the disc is not present in the drive, the copy that was "saved" appears to be a bit-for-bit copy of the entire contents of the CSS encrypted disc, together with whatever data is necessary for successful and complete playback —including the necessary encryption keys.

17. Based on my own observations of the RealDVD software, it appears to bypass multiple important technological restrictions imposed by CSS by (a) allowing the creation of permanent playable and viewable copies of any DVD placed in the drive, and (b) playing those copies even when there is no DVD drive attached to the computer with which to initiate and successfully complete the player authentication process.

18. Ordinarily, a consumer wishing to copy a CSS-protected DVD using an unlicensed program capable of copying DVDs would not be able to "unlock" a DVD drive containing CSS-protected data with that program, and thus not be able to access the contents of a protected DVD. However, RealDVD uses the

authentication protocols it obtained by becoming a licensee of CSS, thus enabling a consumer to make a copy of the protected movie content. RealDVD, by virtue of knowing the authentication protocols is able to "unlock" the DVD drive, and access the full CSS protected content.

19. Ordinarily, a consumer who succeeded, by using an unlicensed program, in gaining unauthorized access only to the CSS encrypted content without first successfully completing the required authentication process with the drive would still be faced with the further technical challenge of causing the drive to provide access to the protected "content key" contained in the lead-in area of the DVD. This is because drives also do not normally permit software from accessing the lead-in area without first successfully completing the authentication process. Without further effort to defeat the method by which the drive limits access to the protected content key, any copies made of the video files on the DVD would remain encrypted and thus be unplayable. As a licensed DVD player, RealDVD, however, is able to successfully complete the authentication process and is then granted access to data in the "lead-in area" of a protected DVD. As described previously, such access is normally granted only to authorized players as determined by the successful outcome of the authentication process, so that programs, which may include unauthorized "copy" functions, will be unable to produce a decryptable and playable copy of a DVD. RealDVD, however, uses the authentication information it obtained from DVD CCA to authenticate and then access the lead-in area and transfer the key data to a user's hard drive along with the CSS protected content.

20. Ordinarily, a DVD marked with the "NeverCopy" signal would not be copied, as the relevant hardware and software would abide by the expressed intent of the content-owner. RealDVD ignores this code, and thus permits users to make persistent, playable copies of DVD marked in such a way as to be specifically unauthorized for copying.

21. Finally, RealDVD does not appear to engage in any authentication with the DVD drive before permitting users to play the previously copied CSS-protected files. By eliminating the DVD drive's role in authentication of the player software, each time it plays a movie it has previous copied, the RealDVD program bypasses entirely the authentication or "locking" mechanisms designed to control unauthorized access to protected DVDs. RealDVD can be used to create perfect playable copies of protected DVDs on the computer system's hard disk drive. RealDVD will play back these copies even when the DVD drive is disconnected from the computer and thus does not initiate or complete the authentication process that is an important element of the CSS system of protection.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on this 29th day of September, 2008.

Alan Bell

Dr. Alan E. Bell