

1 JAMES A. DiBOISE, State Bar No. 83296
 Email: jdiboise@wsgr.com
 2 LEO P. CUNNINGHAM, State Bar No. 121605
 Email: lcunningham@wsgr.com
 3 COLLEEN BAL, State Bar No. 167637
 Email: cbal@wsgr.com
 4 MICHAEL A. BERTA, State Bar No. 194650
 Email: mberta@wsgr.com
 5 TRACY TOSH LANE, State Bar No. 184666
 Email: ttosh@wsgr.com
 6 WILSON SONSINI GOODRICH & ROSATI
 Professional Corporation
 7 One Market Street
 Spear Tower, Suite 3300
 8 San Francisco, CA 94105

9 Attorneys for Plaintiffs and
 Counterclaim Defendants
 10 REALNETWORKS, INC. and
 REALNETWORKS HOME
 11 ENTERTAINMENT, INC.

12 UNITED STATES DISTRICT COURT
 13 NORTHERN DISTRICT OF CALIFORNIA

14 REALNETWORKS, INC., a Washington
 Corporation; and REALNETWORKS HOME
 15 ENTERTAINMENT, INC., a Delaware
 corporation,

16 Plaintiffs,

17 v.

18 DVD COPY CONTROL ASSOCIATION, INC., a
 19 Delaware nonprofit corporation, DISNEY
 ENTERPRISES, INC., a Delaware corporation;
 20 PARAMOUNT PICTURES CORP., a Delaware
 corporation; SONY PICTURES ENTER., INC., a
 21 Delaware corporation; TWENTIETH CENTURY
 FOX FILM CORP., a Delaware corporation; NBC
 22 UNIVERSAL, INC., a Delaware corporation;
 WARNER BROS. ENTER. INC., a Delaware
 23 corporation; and VIACOM, Inc., a Delaware
 Corporation,

24 Defendants.
 25

Case Nos. C08 04548 MHP;
 C08 04719 MHP

**DECLARATION OF MATTHEW A.
 BISHOP, PH.D. IN SUPPORT OF
 REALNETWORKS, INC. AND
 REALNETWORKS HOME
 ENTERTAINMENT, INC.'S
 OPPOSITION TO MOTION FOR
 PRELIMINARY INJUNCTION**

26
 27 AND RELATED CASES
 28

BISHOP DEC ISO REAL'S OPPOSITION TO
 PRELIM. INJUNCTION MOTION
 CASE NOS: C08 04548 MHP; C08 04719
 MHP

1 I, Matthew A. Bishop, declare:

2 1. I am a professor of computer science in the Department of Computer Science at
3 the University of California at Davis, one of the most preeminent such departments in the United
4 States. I and my colleagues at the University of Davis have been recognized for our work in
5 computer security by, among other entities, the United States Department of Defense. I am also
6 the co-director of the Computer Security Laboratory at Davis, and have spent more than twenty
7 years studying, teaching and writing about computer security and encryption. In 2002 I
8 published a textbook on computer security, *Computer Security: Art and Science*, which
9 addresses, among other things, the so-called "Content Scramble System" ("CSS") that is used to
10 encrypt most DVDs that are commercially released in the United States, and that is at issue in
11 this lawsuit. I consider myself to be an expert on the subject of computer security and if called to
12 testify could and would testify competently to the opinions that are expressed herein.

13 2. I have reviewed an extensive list of materials in this matter, including the CSS
14 documentation at issue in this matter and the source code for as the RealNetworks products at
15 issue in this matter. Some of the materials I have reviewed are set forth in the Exhibit Report of
16 Matthew A. Bishop, Ph.D. (attached hereto as Exhibit A) and the Rebuttal Expert Report of
17 Matthew A. Bishop, Ph.D. (attached hereto as Exhibit B). Ex. A, ¶¶ 15-16; Ex. B, ¶ 6.

18 3. As explained in greater detail in my reports and in my deposition testimony, it is
19 my opinion that the Real Products, namely the RealDVD software program and the Facet
20 hardware DVD player, comply with the CSS License and the associated documents, including
21 the General Specifications, Technical Specifications and Procedural Specifications. The Real
22 Products implement all of the steps required by the CSS documentation in the order and at the
23 time required. The Real Products comply with all of the restrictions contained in the CSS
24 documentation. The Real Products protect the DVD video content, CSS keys and CSS
25 algorithms using the methods specified by the CSS documentation. The Real Products maintain
26 all of the CSS protections for DVD content.

27 4. The Real Products also provide extensive protection for DVD content in addition
28 to the CSS protection that the products maintain. Namely, the Real Products use a form of

1 encryption called Advanced Encryption Standard using Cipher Block Chaining with a 128-bit
2 key ("AES-128"). This method of encryption as of yet has no known cryptographic weaknesses.
3 By contrast, the CSS encryption, which the Real Products faithfully maintain, was broken
4 approximately a decade ago.

5 5. Additional opinions I have developed over the course of this matter are set forth
6 in the expert reports attached to this declaration. Exhibits A and B are true and correct copies of
7 those reports.

8
9 I declare under penalty of perjury under the laws of the State of California and the United
10 States of America that the foregoing is true and correct of my own personal knowledge, and that
11 this declaration is executed this 19 day of March, 2009 at Davis, California.

12 

13 _____
14 Matthew A. Bishop
15
16
17
18
19
20
21
22
23
24
25
26
27
28