RICHARD R. WIEBE (SBN 121156)
2140 Ninth Avenue
San Francisco, CA 94116
Telephone: (415) 505-8793
Facsimile: (240) 282-7297

THOMAS E. MOORE III (SBN 115107)
TOMLINSON ZISKO MOROSOLI & MASER LLP
200 Page Mill Road, Second Floor
Palo Alto, CA 94306
Telephone: (650) 325-8666
Facsimile: (650) 324-1808

ALLONN E. LEVY (SBN 187251)
HS LAW GROUP
210 N. Fourth St., Second Floor
San Jose, CA 95112
Telephone: (408) 295-7034
Facsimile: (408) 295-5799

ROBIN D. GROSS (SBN 200701)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Defendant ANDREW BUNNER

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SANTA CLARA

DVD COPY CONTROL ASSOCIATION, INC.,
Plaintiff,
v.

ANDREW THOMAS MCGLAUGHLIN; ANDREW BUNNER; et al.,
Defendants.

Case No CV - 786804

DECLARATION OF COMPUTER SCIENTIST ROLAND PARVIAINEN

IN SUPPPORT OF DEFENDANT ANDREW BUNNER'S MOTION FOR SUMMARY JUDGMENT

I, Roland Parviainen, declare:

1. I am an instructor in the Computer Science and Electrical Engineering Department of Luleå University of Technology in Luleå, Sweden. I received my M.S. degree in Computer Science in 1999 from Luleå University and since that time have been a graduate student in the Ph.D. program in the Computer Science and Electrical Engineering Department at the University.
2. I have taught the Computer Security course three times for the Computer Science and Electrical Engineering Department of Luleå University.
3. I most recently taught the course in Computer Security in the Spring Term of 2001. As part of my course, I taught my students how the Content Scrambling System ("CSS") encrypts and decrypts DVD movie disks.
4. Information about CSS is freely available within the computer science community. In preparing to teach my Computer Security course, I had no difficulty in obtaining from sources on the Internet the information required to understand the CSS algorithms and keys and to understand how those algorithms and keys are used to encrypt and decrypt DVD movies. These sources include Frank A. Stevenson's paper "Cryptanalysis of Contents Scrambling System" as well as source code for various DVD decryption programs. These decryption programs include "DeCSS," a program that decrypts DVD movie disks by implementing the CSS decryption algorithms and keys, as well as other programs that are functionally equivalent but instead exploit weaknesses in the CSS algorithms to decrypt the movie data without replicating the CSS decryption process. The source code available on the Internet for these programs reveals how the CSS algorithms and keys work.

5. I use CSS in my Computer Security course as an example of how not to design an encryption system. CSS is an inherently weak encryption system that can easily be attacked. It has a weak algorithm, relatively short (40-bit) keys that are vulnerable to brute-force attack, and in the case of software DVD players the player key is stored in the computer's memory.

I, ROLAND PARVIAINEN, declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: ____________________ ___________________________

Roland Parviainen