RICHARD R. WIEBE (SBN 121156)
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone:  (415) 433-3200
Facsimile:  (415) 433-6382

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., Suite 201
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.,<br>Plaintiff,<br>v.<br><br>ANDREW THOMAS MCLAUGHLIN; ANDREW BUNNER; et al.,<br>Defendants. | Case No. CV - 786804<br><br>**DECLARATION OF COMPUTER SCIENTIST GREGORY KESDEN**<br><br>**IN SUPPPORT OF DEFENDANT ANDREW BUNNER'S MOTION FOR SUMMARY JUDGMENT** |

I, Gregory Kesden, declare:

1. I am a Lecturer in the Computer Science Department of Carnegie Mellon University in Pittsburgh, Pennsylvania. Among the courses I teach is the department's course in Operating System Design and Implementation. This course is one of the core courses of the Computer Science Department and is the department's most intensive course; it receives 18 units of credit while all other courses receive 12 units or fewer.
2. Issues of computer security and protection, including an introduction to cryptography, are an integral part of a modern operating systems course – and are becoming a more compelling issue each day. All of the major operating systems texts include coverage of this area.
3. As part of my course in Operating System Design and Implementation, I teach my students about information security and protection schemes and the potential vulnerabilities of such schemes. I also teach them about the ways in which reverse engineering is used to enable programs and data to operate compatibly with many different operating systems. In my teaching, I illustrate these concepts using information about the Content Scrambling System ("CSS") used to encrypt DVD movie disks.
4. Last fall I reorganized my Operating System Design and Implementation course to increase the lecture time of the course. The additional lecture time was used to expand the course's coverage of protection and security, networks, and the implementation of the operating system Linux, as well as other areas. As part of my overall revision of the course, I introduced material about CSS. Attached as Exhibit A are my lecture notes and slides I used when I taught CSS's algorithms and keys as part of my Operating System Design and Implementation course in the Fall 2000 Term. These materials are also available on the Internet at http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/index.html.
5. I selected CSS because it is a simple, understandable example of a stream cipher that exhibits some classic cryptographic techniques. Additionally, it is a useful example because it has some well-known and reasonably understandable vulnerabilities and exploits. CSS is a weak encryption system vulnerable to a number of different

cryptological attacks. By teaching how the CSS algorithms and keys operate, I am able to demonstrate how these attacks function. Students are always excited to learn about weaknesses in real-world systems – it makes them feel more expert than the experts. But, beyond that, it helps drive home a very important lesson for future systems developers – cryptography is hard and the process of developing a cryptosystem should be careful and the system thoroughly validated before it is implemented.

6. CSS, DeCSS, and other DVD descrambling programs also illustrate concepts of interoperability—the use of computer data and programs with many different operating systems. For example, because no authorized DVD player was available for the popular Linux operating system, a version of DeCSS as well as other DVD descrambling programs have been created for Linux. Without these programs, it was impossible to play authorized, original DVD movie disks on Linux computers.
7. I also gave a lecture about CSS and DeCSS at the University of California, San Diego, in the Spring of 2001.
8. CSS and its algorithms and keys are widely known in the computer science community, as are DeCSS and other DVD decryption programs. I was able to find on the Internet the information about CSS and DVD decryption I needed for my course. For example, Frank Stevenson's well-known paper analyzing CSS, a copy of which is attached as Exhibit B, is readily available on the Internet. DVD decryption information is also available in more tangible forms as well. Attached as Exhibit C are photographs of a DVD decryption program (in the Perl computer language) printed on self-adhesive stickers which were widely posted on the Carnegie Mellon University campus.

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

Dated: ___________________ __________________________

Gregory Kesden