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

CINDY A. COHN (SBN 145997)
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 MCLAUGHLIN; ANDREW BUNNER; et al., Defendants.	Case No. CV - 786804 **DECLARATION OF PROFESSOR EDWARD W. FELTEN** **IN SUPPPORT OF DEFENDANT ANDREW BUNNER'S MOTION FOR SUMMARY JUDGMENT**

I, Professor Edward W. Felten, declare:

I. Introduction

1. My name is Edward W. Felten. I am a tenured Associate Professor of Computer Science at Princeton University, and I am Director of Princeton's Secure Internet Programming Laboratory. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993, and my B.S. in Physics from the California Institute of Technology in 1985. I have been on the faculty at Princeton for about eight years.

2. For the 2001-2002 academic year, I am on sabbatical leave from Princeton, at the Center for Internet and Society at Stanford Law School. The Center focuses on interactions between technology and the law. I chose to spend my sabbatical year at the Center because of my increasing concern over the impact of new laws and court decisions on technologists. Cases like this one affect the environment in which legitimate computer security researchers and practitioners work. I myself have been restricted in my work by the Digital Millennium Copyright Act, as I describe in ¶ 11 below.

3. My main area of research and teaching is computer security, and my other research interests include operating systems, computer networks, and Internet software. I have published more than fifty papers in the research literature, and am the co-author of two books.

4. At Princeton I have created and taught courses on Information Security, Applied Cryptography, and Distributed Computing and Networking.

5. I have received a number of awards for my research, including a National Young Investigator award from the National Science Foundation, and an Alfred P. Sloan Foundation Fellowship. I have received Outstanding Paper or Best Paper awards at two conferences: in 1997 at the Symposium on Operating Systems Principles, the most prestigious academic conference on operating systems, and in 1995 at SIGMETRICS, the most prestigious conference on computer system performance analysis. I have given numerous special and invited talks at academic conferences.

6. I am the primary computer science expert witness for the U.S. Department of Justice in the ongoing antitrust case against Microsoft, *United States v. Microsoft.* In that capacity, I testified twice at trial and also filed a lengthy declaration in the remedy phase of that proceeding. I also advised the Justice Department extensively during the recently concluded settlement negotiations in that case.

7. I have also worked extensively with law enforcement agencies. I assisted the U.S. Attorney's office and the FBI with the "Melissa virus" case and a few other matters.

8. My research has been funded by government agencies, including the National Science Foundation and the Defense Advanced Research Projects Agency, and by industrial grants or gifts from IBM, Intel, Microsoft, Merrill Lynch, Sun Microsystems, Telcordia, and Trintech.

9. I have been appointed to advisory boards and study panels by industrial, professional, and governmental organizations. Sun Microsystems, Inc. appointed me to its Java Security Advisory Council, and I serve on Technical Advisory Boards for several other companies. The Institute for Defense Analyses[1], working in conjunction with the U.S. Department of Defense, chose me to serve in the Defense Science Study Group, and I obtained a U.S. "Secret" security clearance for that purpose. The Defense Advanced Research Projects Agency (DARPA), which is the main research arm of the Department of Defense, appointed me to its Information Science and Technology advisory board. The National Research Council (which consists of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine) appointed me to its study committee on "Fundamentals of Computer Science." The Association for Computing Machinery (ACM), which is the leading international professional society for computer

[1] The Institute for Defense Analyses is a nonprofit corporation whose purpose is to promote national security and the public interest and whose primary mission is to assist the Office of the Secretary of Defense, the Joint Chiefs of Staff, the unified military commands, and defense agencies in addressing important national security issues, particularly those requiring scientific and technical expertise.

scientists, appointed me to its Advisory Committee on Security and Privacy. I also serve as the moderator of the ACM Forum on Legal Regulation of Technology.

10. My research has been covered extensively in the national press. I have been quoted or profiled on numerous occasions in publications such as the New York Times, the Washington Post, the Wall Street Journal, and Newsweek.

11. I have been personally affected in my academic work by the uncertainty and restrictions generated by the application of new laws and court decisions to the field of computer science. Last year, I led a team of researchers who performed research on a set of proposed digital music copy protection schemes. On the eve of presenting and publishing our results on the significant flaws of these schemes at an academic conference, the Recording Industry Association of America (RIAA) and others threatened to sue us under the Digital Millennium Copyright Act (DCMA). They demanded the right to censor our research paper and our lecture. The chilling effect of this litigation threat caused us to initially withhold publication of our results and cancel the lecture rather than risk violating the DCMA. Because of the importance of ensuring the freedom of researchers to publish the results of their research, we brought a federal court action for declaratory relief. The RIAA and the other defendants subsequently stated they would not sue us under the DCMA, and so we published a paper and gave a lecture on our research at another scientific conference last August. The RIAA and the other defendants still claim a right to censor our further writing and speech on the topic, so our declaratory relief action is still pending.

II. CSS Is Not A Secret

12. I am familiar with the “Content Scrambling System” (“CSS”) used to encrypt DVD movie disks. I understand that Plaintiff claims that the CSS algorithm and its keys remain a secret that is not generally known. As an active participant in the computer security research community, I can state with confidence that this claim is wrong.

13. It is wrong for at least two reasons. First, DeCSS has been, and continues to be, widely available from sources other than Mr. Bunner. Second, even independent of the

availability of DeCSS, both the CSS algorithm itself, and methods for determining the keys it uses, are now widely known.

III. DeCSS Continues To Be Widely Available

14. The source code for DeCSS is available at many places on the Internet. These can be found easily with a search engine. As I was writing this paragraph, I stopped to do a Web search for the term “DeCSS source code” on the Google search engine. It took me less than fifteen seconds to find a copy of DeCSS.

15. Some DeCSS Web sites are widely known and discussed. For example, Dr. David Touretzky at Carnegie Mellon University runs a site called “Gallery of CSS Descramblers,” at http://www.cs.cmu.edu/~dst/DeCSS/Gallery, which contains code and procedures for descrambling CSS, expressed in many forms and media, including several computer languages. This site has been mentioned many times in court testimony and in the popular press. Its existence is common knowledge in the computer security research community.

16. In my everyday discussions with students, I have observed that many computer science students know what DeCSS is and know how to get it.

IV. The CSS Algorithm And The Keys It Uses Are Widely Known

17. Even independent of DeCSS, the details of the CSS algorithm are available on the Internet and are widely known. For example, a well-known paper by Frank Stevenson (entitled “Cryptanalysis of Contents Scrambling System”) describes how CSS works and what its weaknesses are. This paper continues to be available on several Web sites. It can be found in seconds by doing a Web search on its title, or on its author’s name. A search for the term “Frank Stevenson” on the Google search engine returns many links to Stevenson’s paper, including one at http://www.cs.cmu.edu/~dst/DeCSS/FrankStevenson/analysis.html.

18. Stevenson’s research is widely known and discussed in the computer security research community.

19. For example, not long after Stevenson’s paper was published, I gave an informal seminar talk about it at Princeton. The audience was a room full of faculty, graduate

students, and undergraduates. I have also used DeCSS, CSS, and Stevenson's results as an example in one of the lectures of my senior-level Information Security course.

20. Although Stevenson's paper does not provide the CSS cryptographic keys, it describes methods by which those keys can be determined. These methods are well within the means and expertise of a typical computer science student, and do not require any rare tools: an ordinary personal computer and a few DVDs suffice.

21. As these facts demonstrate, neither CSS nor the keys it uses remain secret.

V.   CSS and its Keys Would Inevitably Have Become Public

22. I understand that Plaintiff chose to allow wide distribution of DVD player computer software programs, running on personal computers, implementing CSS and containing valid keys. This decision to authorize software DVD players and not to limit DVD players to only hardware versions made it virtually inevitable that knowledge of CSS and its keys would become public.

23. Personal computer software is inherently amenable to reverse engineering. The tools to do this reverse engineering are widely available at little or no cost and run on ordinary personal computers.   There are, at the very least, hundreds of thousands of people worldwide who have the skill to use them.

24. Reverse engineering tools for personal computer software are so good, and so widely available, because they have other valuable uses, especially in "debugging" software. Programmers spend many hours debugging the software they have written (i.e., diagnosing its malfunctions in order to fix them). Debugging is essentially the process of reverse-engineering your own software, so that you can figure out how its behavior differs from the behavior you desire. Any skilled programmer is good at debugging; and debugging is just reverse engineering. Applying the same tools, and many of the same methods, to software implementations of CSS, would yield an understanding of how CSS works.

25. Although some products exist that claim to "harden" software against reverse engineering, these products generally impair the performance of the "hardened" software,

and have only a limited practical effect against a skilled reverse engineer. Indeed, a recent discovery in theoretical computer science[2] proves that it is *impossible* to build a tool that effectively hardens arbitrary programs.

26. Because so many people have the skills and tools to reverse-engineer programs, Plaintiff's decision to authorize the release of CSS in software form made it virtually inevitable that somebody, somewhere, would reverse engineer it. It is hard to imagine that Plaintiff did not foresee this.

27. Once CSS became public knowledge, its keys inevitably also would have become public knowledge. This is true because the designers of CSS made the "rookie mistake" of using only a forty-bit key. It is common knowledge that use of a forty-bit key allows an easy brute-force search to determine the key, given a sample of encrypted material (e.g., a DVD movie disk). It is virtually impossible to imagine that Plaintiff did not realize this.

28. In fact, because the designers of CSS made the additional "rookie mistake" of using a home-grown cryptosystem rather than an "industrial-strength" one, it was not even necessary to search the entire 40-bit "key space" (i.e., the mathematical universe of all possible 40-bit numbers) to determine the working keys. Frank Stevenson was apparently the first to notice this, but the flaws in CSS were not terribly difficult to find. Finding the flaws in CSS would in fact make a good homework problem for a course in cryptography. It seems unlikely that Plaintiff could have done a due-diligence evaluation of CSS without learning of these additional flaws.

29. These facts demonstrate that Plaintiff's decision to allow personal computer software implementations of CSS made it virtually inevitable that CSS and its keys would become public knowledge. From my experience in the academic, commercial, government, and national security arenas of computer science, I know that this is not how businesses and individuals normally treat valuable information they desire to keep secret. In my view, the

[2] "On the (Im)possibility of Obfuscating Programs," by Barak, et al., Proceedings of the 21st International Conference on Cryptology, Santa Barbara, August 2001.

actions taken by Plaintiff cannot be considered reasonable efforts to maintain the secrecy of the CSS algorithm and keys.

I, EDWARD W. FELTEN, declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated: ____________________ ___________________________

Edward W. Felten