1 RICHARD R. WIEBE (SBN 121156)
   425 California Street, Suite 2025
2 San Francisco, CA 94104
3 Telephone: (415) 433-3200
   Facsimile: (415) 433-6382
4

5 THOMAS E. MOORE III (SBN 115107)
   TOMLINSON ZISKO MOROSOLI & MASER LLP
6 200 Page Mill Road, Second Floor
   Palo Alto, CA 94306
7 Telephone: (650) 325-8666
   Facsimile: (650) 324-1808
8

9 ALLONN E. LEVY (SBN 187251)
   HS LAW GROUP
10 210 N. Fourth St. Second Floor
   San Jose, CA 95112
11 Telephone: (408) 295-7034
12 Facsimile: (408) 295-5799

13 CINDY A. COHN (SBN 145997)
   ROBIN D. GROSS (SBN 200701)
14 ELECTRONIC FRONTIER FOUNDATION
15 454 Shotwell Street
   San Francisco CA 94110
16 Telephone: (415) 436-9333
17 Facsimile: (415) 436-9993

18 Attorneys for Defendant ANDREW BUNNER

19   SUPERIOR COURT OF THE STATE OF CALIFORNIA

20   COUNTY OF SANTA CLARA

21

22 | DVD COPY CONTROL ASSOCIATION, | Case No. CV - 786804 |
   INC., | **DATE: January 29, 2002**
23 | Plaintiff, | **TIME: 9:00 a.m.**
24 | v. | **DEPT.: 2**
                                   | **HONORABLE WILLIAM J. ELFVING**
25 | ANDREW THOMAS MCLAUGHLIN;
   | ANDREW BUNNER; et al., | **DEFENDANT**
26 | Defendants. | **ANDREW BUNNER'S**
27 | **STATEMENT OF UNDISPUTED**
                                   | **FACTS IN SUPPORT OF HIS MOTION**
28 | **FOR SUMMARY JUDGMENT**

1. The Content Scrambling System ("CSS") is an encryption system for DVD movie disks consisting of algorithms and keys.	12/20/00 Amended Submission of Plaintiff DVD Copy Control Assoc., Inc., Pursuant to § 2019(d); Complaint ¶ 30.
2. The alleged trade secrets that plaintiff DVD Copy Control Association, Inc. ("DVD CCA") alleges in this action were misappropriated by defendant Andrew Bunner are the algorithms and keys used by CSS as described in Plaintiff DVD CCA's 12/20/00 Amended Submission Pursuant to § 2019(d), and the Matsushita Electrical Industrial Co., Ltd. CSS documentation included as Exhibit A thereto.	12/20/00 Amended Submission of Plaintiff DVD Copy Control Assoc., Inc., Pursuant to § 2019(d).
3. The DVD decryption program known as DeCSS was published on the Internet in October 1999.	Complaint ¶ 45.
4. The DeCSS computer program exists in various source code and object code versions, including decss.exe, decss-source, and css-auth.	Prof. Wagner Decl. ¶¶ 8, 18; Dr. Touretzky Decl. ¶ 2.
5. The DeCSS computer program remains available in at least at hundreds of locations on the Internet, in both source code and object code versions.	Prof. Wagner Decl. ¶¶ 6-21; Dr. Touretzky Decl. ¶¶ 13-15, 18-23; Prof. Felten Decl. ¶¶ 14-15.
6. The DeCSS computer program remains available in at least more than 200	Prof. Wagner Decl. ¶¶ 6-21.

hundred locations on the Internet in source code versions.	
7. The DeCSS computer program remains available in at least more than 160 locations on the Internet in object code versions.	Prof. Wagner Decl. ¶¶ 6-21.
8. Other DVD software players have been created since the creation of DeCSS that also disclose the CSS algorithms and keys, including Videolan, developed at the École de Paris; Ogle, developed at Chalmers University in Sweden; and Xine.	Prof. Wagner Decl. ¶¶ 22-25; Dr. Touretzky Decl. ¶¶ 11, 24-25, 30.
9. These other DVD software players are available on the Internet.	Dr. Touretzky Decl. ¶¶ 11, 24-25, 30; Prof. Wagner Decl. ¶¶ 22-25.
10. Numerous additional programs performing the CSS descrambling function have been created in a variety of programming languages.	Dr. Touretzky Decl. ¶¶ 14-15, 29.
11. MIT's journal *Technology Review* and *Wired Magazine* have published one of these DVD descrambling programs, and the *Wall Street Journal* published one of the CSS master keys.	Dr. Touretzky Decl. ¶¶ 10, 29 & Exs. A, B, C.
12. DVD descrambling programs have been publicly posted on adhesive stickers.	Kesden Decl. ¶ 8 & Ex. C.
13. Dr. Touretzky of Carnegie Mellon	Dr. Touretzky Decl. ¶¶ 14, 18.

University maintains a "Gallery of CSS Descramblers" web site (http://www.cs.cmu.edu/~dst/DeCSS/Gallery) on the Internet.	
14. The CSS algorithms and keys are available both at the Gallery of CSS Descramblers and elsewhere in the form of computer source code, narrative descriptions, mathematical descriptions, and graphical, animated, and musical renderings.	Dr. Touretzky Decl. ¶¶ 13-25, 28.
15. CSS and its algorithms and keys have been the subject of research, discussion, and teaching worldwide within the computer science community, both academic and non-academic.	Prof. Felten Decl. ¶¶ 12-13, 16-21; Prof. Wagner Decl. ¶¶ 28-33; Dr. Touretzky Decl. ¶¶ 26-32; Kesden Decl. ¶ 4-8; Parviainen Decl. ¶¶ 1-5.
16. Professor Felten at Princeton has taught a seminar on CSS and has taught CSS and DeCSS in his Information Security course.	Prof. Felten Decl. ¶ 19.
17. Professor Wagner has taught CSS in his Security in Computer Systems course at the University of California, Berkeley.	Prof. Wagner Decl. ¶ 28.
18. Computer Scientist Kesden teaches CSS as part of his course on operating systems at Carnegie Mellon University, and his course materials describing the operation	Kesden Decl. ¶¶ 1-5 & Ex. A.

DEF. BUNNER'S STATEMENT OF UNDISPUTED FACTS IN SUPPORT OF HIS MO. FOR SUM. JUDGMENT

of CSS are posted in the Gallery of CSS Descramblers.	
19. Computer Scientist Kesden has lectured on CSS at the University of California, San Diego.	Kesden Decl. ¶ 7.
20. MIT has held a seminar on CSS and DeCSS.	Dr. Touretzky Decl. ¶ 29.
21. Computer Scientist Parviainen of Sweden's Luleå University of Technology teaches CSS in his Computer Security course.	Parviainen Decl. ¶ 5.
22. Computer Scientist Parviainen of Sweden's Luleå University of Technology teaches CSS in his Computer Security course as an example of how not to design an encryption system.	Parviainen Decl. ¶ 5.
23. Computer Scientist Kesden teaches CSS in his operating systems course at Carnegie Mellon University as an example of how not to design an encryption system.	Kesden Decl. ¶ 5.
24. Professor Wagner has taught CSS in his Security in Computer Systems course at the University of California, Berkeley as an example of how not to design an encryption system.	Prof. Wagner Decl. ¶¶ 28-29.
25. CSS algorithms and keys are available	Prof. Wagner Decl. ¶ 26.

from Harvard University and Case Western Reserve University web sites.	
26. Cryptographer Frank Stevenson's technical paper describing the CSS algorithms and keys, "Cryptanalysis of Contents Scrambling System," is widely known in cryptographic circles and is available on the Internet.	Prof. Felten Decl. ¶¶ 17-20; Dr. Touretzky Decl. ¶¶ 11-12; Kesden Decl. ¶ 8 & Ex. B; 1/7/00 Stevenson Decl. ¶¶ 15-18.
27. In his paper, Stevenson presents a method for deriving every possible CSS master key.	Dr. Touretzky Decl. ¶ 12; Kesden Decl. Ex. B.
28. Stevenson in his paper also presents a method for deriving the title keys on a movie disc without the use of a master key.	Dr. Touretzky Decl. ¶ 12; Kesden Decl. Ex. B.
29. There is nothing secret about CSS and its algorithms and keys.	Prof. Felten Decl. ¶ 12; Prof. Wagner Decl. ¶ 27; Dr. Touretzky Decl. ¶¶ 31-32, Kesden Decl. ¶ 8; Parviainen Decl. ¶ 4.
30. The CSS algorithms and keys are widely and readily available.	Prof. Felten Decl. ¶ 12; Prof. Wagner Decl. ¶ 27; Dr. Touretzky Decl. ¶¶ 31-32, Kesden Decl. ¶ 8; Parviainen Decl. ¶ 4.
31. It is DVD CCA's position that "Plaintiff cannot reasonably be expected to perform this process to verify the contents of thousands of web sites claiming to be posting Plaintiff's trade secrets."	10/3/00 Plaintiff's Highly Confidential Supplemental Ans. & Objs. To Def. Andrew Bunner's First Set of Interrogs., at 4.
32. DVD CCA to date has named only 24	10/9/01 Case Management Conference

defendants in this action and has served 22 of them.	Questionnaire of DVD CCA.
33. DVD CCA has not named and served as defendants the publishers of the 72 web sites identified in its interrogatory answers as disclosing information about CSS algorithms and keys.	10/3/00 Plaintiff's Highly Confidential Supplemental Ans. & Objs. To Def. Andrew Bunner's First Set of Interrogs., at 3-5; 8/10/00 Plaintiff's Highly Confidential Ans. & Objs. To Def. Andrew Bunner's First Set of Interrogs., at 3; 10/9/01 Case Management Conference Questionnaire of DVD CCA; Complaint.
34. DVD CCA and its predecessors in interest have licensed CSS for use in software DVD players for computers.	Complaint ¶ 35.
35. Licensed CSS software DVD players necessarily contain in software form the CSS algorithms and keys.	Prof. Felten Decl. ¶ 22; Prof. Wagner Decl. ¶ 35.
36. The distribution of licensed CSS DVD players in software form made it more likely that CSS would be publicly disclosed.	Prof. Felten Decl. ¶¶ 22-29; Prof. Wagner Decl. ¶¶ 29, 34-40.
37. The weak encryption techniques used in CSS made it more likely that the CSS algorithms and keys would be publicly disclosed.	Prof. Felten Decl. ¶¶ 27-28; Prof. Wagner Decl. ¶ 29; Dr. Touretzky Decl. ¶¶ 11-12, 26; Kesden Decl. ¶ 5; Parviainen Decl. ¶ 5.
38. Section 5.2 of the CSS Interim License Agreement provides: "(h) <u>Confidentiality Exceptions</u>. The confidentiality	CSS Interim License Agreement, ¶ 5.2(h), reproduced at 1/13/00 Hoy Reply Decl., Ex. C.

restrictions contained in Sections 5.2(a), (b) and (c) herein shall not apply to information that Licensee can demonstrate: (i) is either Confidential or Highly Confidential Information which is or becomes generally known to the public through no breach of Licensee's obligations owed to *[Blank]* hereunder and which *[Blank]* failed to remove from public availability or to enjoin such public disclosure within ninety (90) days after the date such information is or becomes generally known as set forth above; . . ."	
39. Defendant Andrew Bunner had nothing to do with the creation or programming of DeCSS or any other DVD descrambling program.	Bunner Decl. ¶ 2.
40. Mr. Bunner had nothing to do with the reverse engineering or technical analysis of CSS that preceded the creation of DeCSS.	Bunner Decl. ¶ 3.
41. Mr. Bunner was not involved in the original publication of DeCSS or any other DVD descrambling program on the Internet.	Bunner Decl. ¶ 4.
42. Mr. Bunner first learned of DeCSS after CSS had been reverse engineered and after DeCSS had been created and	Bunner Decl. ¶ 5.

published on the Internet in October 1999.	
43. After the creation and publication on the Internet of DeCSS, Mr. Bunner then downloaded a copy of DeCSS from an unrestricted, publicly available web site on the Internet and placed it on his personal web site.	Bunner Decl. ¶ 6.
44. In December 1999, before being served with the summons and complaint in this action, Mr. Bunner spoke by telephone with an attorney for DVD CCA.	Bunner Decl. ¶ 7.
45. Mr. Bunner immediately removed DeCSS from his web site server during his telephone conversation with DVD CCA's attorney in December 1999, has not disclosed or distributed DeCSS since that time, and has observed the terms of the preliminary injunction.	Bunner Decl. ¶ 7.

Dated: November 28, 2001   Respectfully submitted,

                                             _____

                                             Richard R. Wiebe
                                             Attorney for Defendant
                                             Andrew Bunner

**DEF. BUNNER'S STATEMENT OF UNDISPUTED FACTS IN SUPPORT OF HIS
MO. FOR SUM. JUDGMENT**