Grayson Barber (GB 0034)
Grayson Barber, L.L.C.
68 Locust Lane
Princeton, New Jersey 08540
(609) 921-0391

Frank L. Corrado (FLC 9895)
Rossi, Barry, Corrado & Grassi
2700 Pacific Avenue
Wildwood, NJ 08260
(609) 729-1333
Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

EDWARD W. FELTEN; BEDE LIU; SCOTT A. CRAVER; MIN WU; DAN S. WALLACH; BEN SWARTZLANDER; ADAM STUBBLEFIELD; RICHARD DREWS DEAN; and USENIX ASSOCIATION, a Delaware non-profit non-stock corporation, Plaintiffs vs. RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.; SECURE DIGITAL MUSIC INITIATIVE FOUNDATION; VERANCE CORPORATION; JOHN ASHCROFT, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES; DOES 1 through 4, inclusive, Defendants.	Hon. Garrett E. Brown, Jr. Case No. CV-01-2669 (GEB) Civil Action **DECLARATION OF EUGENE H. SPAFFORD IN OPPOSITION TO JOHN ASHCROFT'S MOTION TO DISMISS**

I, EUGENE H. SPAFFORD, of full age, hereby declare:

1. My name is Eugene H. Spafford. I currently reside in West Lafayette, Indiana.

2. I am a full professor of Computer Sciences at Purdue University, where I also have a courtesy appointment as a full professor of philosophy. I have been on the faculty of Purdue University since 1987. I am also Director of the Center for Education and Research in Information Assurance and Security (CERIAS), considered by many people to be the world's foremost, multidisciplinary academic research group in information security issues.

3. I received my B.A. degree with a double major in Mathematics and Computer Sciences from the State University College at Brockport (1979, NY). I then attended the School of Information and Computer Sciences (now the College of Computing) at Georgia Institute of Technology, where I received my M.S. in 1981, and Ph.D. in 1986. After a year of post-doctoral studies at Georgia Tech, I joined the faculty at Purdue University.

4. I have been involved with both research and practice in computer security and with the social impact of computing for over 20 years. I have been a user of computer networks for the same period of time. I have published over 100 scholarly articles and papers on issues of computer and network security, software engineering, and on computer crime and ethics. I have also co-authored and edited five widely-cited and honored reference books, including "Practical Unix and Internet Security," "Web Security & Commerce," and "The CRC Handbook of Computer Science and Engineering."

5. I am currently the co-chairman of the US Public Policy Committee, USACM, and I am a member of the Board of the Computing Research Association. Over the past few years, I have served in an advisory or consulting capacity on information security and computer crime with several U.S. government agencies and their contractors, including the NSF's CISE division, the FBI, National Security Agency, U.S. Attorney's Office, and the Secret Service. I am currently a member of the Air Force Scientific Advisory Board. I have also been an advisor to

several Fortune 500 firms, and state and national law enforcement agencies around the world. Over the last few years, I have been asked to testify in several hearings before members of Congress, and to meet with President Clinton to discuss information security needs and issues.

6. My service and accomplishments have been recognized by my peers: among other honors, I am a Fellow of the ACM, a Fellow of the AAAS (American Academy for the Advancement of Science), a Fellow of the IEEE (Institute of Electrical and Electronics Engineers), and a recipient of the Computer Society's Golden Core. I have been named to the Upsilon Pi Epsilon and Sigma Xi honor societies. I have been named to the Hall of Fame of the Information Systems Security Association (ISSA), and named as a Certified Information Systems Security professional *honoris causa*. In 2000, I was awarded the National Computer Systems Security Award by US government agencies; the NCSSA award is generally considered the highest award for research, service, and education in information security.

7. I have also been honored for my work as an educator, including receiving the year 2001 William Hugh Murray medal of the National Colloquium for Information System Security Education, and in 2001 receiving Purdue University's two highest awards for teaching: the Charles B. Murphy Award, and being named as a Fellow of the Purdue Teaching Academy.

8. I have extensive experience both in research and in education of information security. I also have extensive experience with information security issues in industry, in national defense, and in law enforcement.

9. A fundamental process of science is to develop hypotheses, create means of testing those hypotheses, and using the results of those tests to increase our body of knowledge. The process of engineering research includes construction of artifacts based on our best available knowledge, stressing those artifacts, and observing how they perform (or fail). From those

observations, we gain new insight into how to construct new artifacts, and new insight into the scientific principles that underlie them. The discipline of computer science combines elements of science and engineering. To make advances, we formulate hypotheses and build systems, then test them to learn more about the underlying principles.

10. Information security, as a sub-field of computing, is concerned with protecting computing resources and the information they contain. Our understanding of threats, and of protection, is not always complete. Therefore, as researchers and practitioners, we often need to use tools and techniques to analyze our systems and software to determine how they are working, to counter malicious behavior, and to improve security. The DMCA interferes with all of these activities, to the detriment of public safety, restricting needed education, and interfering with scholarly research. This will be detailed in the following paragraphs.

11. In commercial practice or national security applications, it is often the case that a computer virus or computer worm will contaminate and damage information processing systems. These are bits of code that insinuate themselves into the software of a running system, altering existing software, and having some undesired effects. To understand the impact of these bits of *malware* (malicious software) and develop remedies and countermeasures, it is necessary to understand what the malicious software does and how it has infiltrated existing software. Sometimes, this malicious software is self-encrypting as a means of thwarting defensive examination.

12. Individuals may also attack systems using toolkits not involving traditional malware. As part of these attacks, system programs may be altered or replaced with other versions that contain hidden code. These "backdoors" allow the attackers to reenter the systems, bypassing normal security controls. The modified code may also contain time-delayed,

destructive code, or code to commit further offenses under remote control. To understand what this code is and does, and to develop remedies and countermeasures, it is necessary to understand what the modified software does and how it works. This malicious software may also be self-encrypting to thwart examination.

13. In both the cases described in paragraphs 11 and 12, it is necessary for scientists to develop and employ forensic tools that decrypt the malicious code, and reverse-engineer it. Without such tools, it is not possible to properly understand and thwart these attacks. Criminals, vandals, terrorists, or other persons of malicious intent may commit these attacks, and it is therefore important to be able to investigate and react to instances of computer abuse. However, if any of these instances of malware or system attacks affects software with copy protection, the DMCA proscribes scientists from the reverse engineering and decryption necessary to investigate and respond to the problem.

14. In addition to the above, the DMCA prevents the development and distribution of forensic tools needed by scientists to investigate and respond to system attacks and malware. Forensic tools include reverse engineering or decryption capabilities. Malicious software and attack tools are creative expression fixed in a tangible form, and thus protected by copyright. These often contain code to prevent reverse engineering and circumvention of various functions. Scientists are proscribed from building important forensic tools because they could be used to circumvent or defeat these copy protections in violation of the DMCA.

15. As a result, the DMCA has had a chilling effect on technologists' ability to produce forensic tools and a chilling effect on scientists interested in performing research in this area. Researchers working in this field, including myself, have limited or altogether stopped development and distribution of forensic tools since the DMCA prohibited their creation; I am

not willing to face the risk of liability, despite the public's compelling need for the forensic technologies I might create.

16. In the regular course of studying software engineering, operating systems, compilers, or a number of other computer science topic areas, instructors often require that students create software as assignments and tools for those assignments. Individuals wishing to add to their own knowledge of these topics outside of structured educational settings will also need to write sample programs and tools. Advanced thesis work and projects also often require development of software tools. For many of these educational exercises, the required software and tools involve reverse engineering. This is required to examine the behavior of the systems and software being used. In many cases — such as in building debuggers or system analyzers — the student project itself includes reverse engineering capability. These tools could be used to circumvent copy protection software if they are used improperly, although that is not the primary reason they are created or distributed. However, as these have no commercially significant market, they are illegal or actionable to develop and distribute under the DMCA.

17. The uncertain threat of a lawsuit has been sufficient to dissuade research in forensics and reverse engineering. Already, academic faculty and amateur researchers are steering away from conducting and publishing research that might result in a suit, creating a significant chilling effect in these scientific disciplines.

18. Requiring the permission of the copyright holder to perform research on the security measures involved, including encryption, means that it is possible for a deployed product to undergo no legal examination because the copyright holder withholds permission. This will likely result in products with weak encryption or poor security being widely marketed — including to government and critical infrastructure operators. However, criminals and extra-

national interests will have no compunction about finding the flaws in that software and exploiting it. One result is a potential increase in the deployment of exploitable products in the US, resulting in a weakening of US national security and increased threats to commerce. Research will continue in other countries where the laws do not mirror the provisions of the DMCA that restrict production and publication of reverse-engineering and decryption technology. As a result, the locus of research in these critical areas may move outside the United States, which would present a threat to national security. (This effect was clearly visible in the 1990s when there were domestic prohibitions on encryption deployment and sale.) We have already seen instances of non-U.S. scientific researchers declaring they will not collaborate or travel to the U.S. to present results because of their fear of the DMCA. Thus, in addition to chilling their speech, the DMCA may well lead to a degradation of the professional effectiveness and collaborative opportunities of security researchers in the U.S.

19. Researchers also require access to a wide array of digital content to improve security and defense capabilities. Without fair use access to digital media, some security applications will take longer to develop and be less robust because research in the development phase will be hampered by inferior and less diverse digital content. For example, researchers are currently assessing various methods of examining digital information to detect steganographic content (hidden messages). This is a laborious procedure that requires constant revision and testing of algorithms that might be used to hide messages inside digital media. The provisions of the DMCA will not dissuade criminals, terrorists and foreign agencies. Therefore, malfeasors may likely choose to embed their encrypted messages and malicious software in copy-protected media precisely because its legal analysis is limited by the DMCA. Thus, because domestic

research is legally constrained, detection and countermeasures needed for U.S. public safety and homeland defense may be less effective.

I declare under penalty of perjury that the foregoing is true and correct and that this declaration is executed in West Lafayette, Indiana on October 23, 2001.

____
EUGENE H. SPAFFORD