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

SUPPLEMENTAL DECLARATION OF SCOTT CRAVER

I, SCOTT CRAVER, of full age, hereby declare:

1. I am one of the Plaintiffs in this action. I am presently a Ph.D. candidate in the

department of Electrical Engineering at Princeton University. My primary area of research is information security, in particular the study of "information hiding." I am a co-author of the book *Information Hiding: Techniques for Steganography and Digital Watermarking*, and have authored and co-authored a number of research papers on the subject of digital watermarks. On August 6, 2001, I signed a Declaration in opposition to the motions to dismiss made by the private Defendants, RIAA, SDMI and Verance, which Declaration was filed with the Court on or about September 10, 2001.

2. This Declaration, which will be submitted in opposition to Defendant John Ashcroft's motion to dismiss, is intended to supplement my earlier Declaration, which I incorporate here in full by this reference. I have read the government's memorandum in support of the motion to dismiss, and I believe that it shows a fundamental factual misunderstanding both with respect to what we did specifically as part of the SDMI research, paper and presentation process, and what we do generally as scientists and academics. I will therefore attempt to set straight the facts. I will also speak further about the forensic music analysis program which I am writing as part of my Ph.D. studies and which I described in my first Declaration.

3. The nature of my particular work in information hiding, and of computer security work in general, necessarily involves both attacks on security systems and defenses against such attacks. In the course of one's work, one cannot usually choose simply to be on one side or the other. This is because we learn, and improve the state of the art, by playing both offense and defense. If someone breaks my security system, I learn from the break (assuming I know about it), and I act accordingly to improve my system. If I break someone else's security system, he learns from the break (assuming he knows about it), and seeks to improve his system accordingly. Additionally, I learn to avoid certain

mistakes in working on my systems.

4. This is what has been described by a number of declarants as the two pillars of security research, synthesis and analysis. See, for example, paragraphs 95 - 104 of Prof. Felten's Declaration in opposition to the private defendants' motions to dismiss. For the process to work, it is essential that it happen in the open, not in secret. When Johnson's analysis results in a break of Smith's security system, the beneficiaries of the knowledge obtained are not just Johnson and Smith, but also Jones, Green and a host of others. In science, we feed off of each other's work, to move forward quickly, rather than wasting time and resources on reinventing the wheel.

5. Essential to this process is not just saying that analysis has resulted in a security system being broken, but proving it with sufficient detail so that others can replicate the attack, determine whether it is valid, and learn from it as much as can be learned. Non-replicable achievements have little value in serious science.

6. The level of detail required for this purpose often cannot be provided within the word or page limitations for scientific papers presented at conferences such as the USENIX Security Symposium, or within the time limitations (typically twenty minutes plus questions) for oral presentations of the highlights of the paper at the conference. In this case, the typical manner of providing the necessary detail is to include in the paper and/or a slide shown during the oral presentation a URL (Uniform Resource Locator) to a web site where interested persons can obtain further detail. If the author of a paper has written a computer program as part of the research process, it is common to provide a URL to the full source code for the program, so that others may examine and study it, and if they choose, download the source code so that they can compile it and run the program. Alternatively,

the author will simply give the program (often e-mailing it) to those who request it.

7. The practice I have described has been my own as well as the general practice in the community. In the past, before the DMCA became law, I wrote computer programs to analyze and break watermarking systems. Other students and researchers asked me for the source code, so that they would not have to spend many hours writing what had been already written. I was, of course, happy to provide the code to people, so that they could perform similar research. Some of these programs were specifically written to circumvent digital watermarks.

8. As I alluded to in paragraph 17 of my first Declaration, we wrote computer programs during the course of the SDMI Challenge, and wrote those programs specifically to circumvent the SDMI technologies, which are a form of access control measures.

9. In the highly peculiar context of the SDMI Challenge we felt comfortable writing programs designed to circumvent access control technologies. SDMI had, after all, invited the public to crack their technologies, and in order to do so, it was necessary to write computer programs designed for that purpose. However, removed from the SDMI Challenge context, I, and I believe the other researchers, would fear the DMCA repercussions of writing such programs, even if the intent ultimately was to strengthen, not weaken, access control technologies. As I have indicated earlier in this Declaration, technology is strengthened by breaking it and then improving it.

10. As I have also mentioned, science is not advanced unless there is adequate proof of the analysis. I was the one who made the oral presentation at the USENIX Security Symposium, and in accordance with standard practice which I have described, normally I would have included in the last slide of my presentation a URL for a web site which had the source code for the programs we wrote.

11. There are at least two reasons why I would have done so. First, bald assertions of achieving an objective do not fly in the scientific community any more than in others. Giving interested persons access to the programs we wrote would have served to prove that we accomplished what we said we accomplished. Second, since some of our programs could be used more generally in the digital watermarking field, it would have furthered science by publishing the full source code for those programs.

12. However, since publishing those programs would have violated the DMCA in our view, and since publication of them at the USENIX Security Symposium would have been outside the peculiar context of the SDMI Challenge, we could not publish the programs. We compromised by including a few snippets of source code for our programs in the SDMI Paper, enough hopefully to show interested persons that we were on the right track. But those snippets simply are not the same as publishing all of our source code for our programs, which we would have done, consistent with scientific practice, in the absence of DMCA constraints. Compare, for example, the snippet of code in the SDMI Paper (Section 3.4, Figure 8, attached to the government's memorandum as Exhibit B) to the full source code for the program called tinywarp.c, which we wrote specifically to circumvent SDMI technology. The full source code will be filed, under seal, as Exhibit 1 to this Declaration. (Figure 8 is not a literal extract from tinywarp.c, since it would have taken up too much space in the paper to extract literally what we wanted to convey. Figure 8 is a highly summarized representation of the logic of tinywarp.c)

13. Our programs "describe[] in detail how to go about circumventing a particular technology," (DOJ Memo, page 17 note 5) and were written for the express purpose of circumventing

the SDMI technologies. What the government may not understand is that this is exactly how science is advanced, and the government's statement that it is possible that making available such programs would be prosecuted can serve only to inhibit progress. The very uncertainty which the government expresses is good reason why we self-censored the presentation and why our dilemma continues today. Do we benefit the scientific community and risk DMCA liability by publishing them, or do we play it safe and deprive the community of whatever we may have accomplished?

14. Tinywarp.c applies a very subtle warping to music, slowing it down and speeding it up so slightly that people cannot perceive the change. The effect is similar to a record player turntable that occasionally spins more quickly, or more slowly, than it is supposed to; but never to such a degree that a listener would notice.

15. In paragraph 31 of my first Declaration, I mentioned a computer program known as Stirmark, which attempts to damage watermarks in computer images. Stirmark is similar in spirit to our program, in that it accomplishes its goal by applying a subtle warping to watermarked images. In the case of images, warping consists of slightly stretching the image's "canvas" in various locations. The watermark is rendered undetectable, because the warping misaligns the watermark relative to the watermark detector. Some watermark detectors fail as a result of this slight miscalibration. More advanced detectors, however, will succeed despite the warping.

16. Had we made this program available to people in its entirety, they would be able to use it on music samples, and verify that it alters music in a very subtle fashion. Furthermore, because sufficiently advanced watermark detectors are not defeated by this program, it can be used in the same way that Stirmark is used: as a benchmark, to test if a watermark system is robust, or too weak to be

trusted.

17. Thus, this computer program is useful to researchers in a number of different ways. First, it communicates the exact method we used to defeat a watermarking system; someone versed in computer programming can read the source code, learning the specifics of our method for altering music. Second, it can be used to replicate our findings, and to confirm our claims that our alteration did not noticeably harm the quality of the watermarked music. Third, this program can be used to test other watermark detectors, to determine if those watermarking systems need to be improved. Providing this code to people, however, could run us afoul of the law, since it was written for the express purpose of circumventing a particular access or copy control technology. Even if others use it as a benchmarking tool, it would still have the primary purpose of attempting to disable watermarks, to determine their strength.

18. Our work during the challenge has led to improved methods of uncovering hidden information in music. This was driven by our efforts to find hidden data in watermarked music provided by SDMI. The opportunity to use various analysis techniques in practice resulted in new and better analysis techniques, and a better understanding of what future scientific development is needed in this field. I regret not being able to learn more from those efforts, and I will regret if we cannot safely add our full analysis to the body of generally available scientific knowledge.

19. If the government can prosecute or if private parties can sue those who write and/or use programs specifically designed to circumvent access or copy control technologies then the scientifically important and growing field of information hiding research will be eviscerated. As in most scientific disciplines, data collection is essential to information hiding research; we do not operate in a vacuum.

But in information hiding research, we collect data precisely by writing and using programs designed to circumvent digital watermarks, among other things. As I stated in paragraph 15 of my first Declaration, we stress them, we overwrite them, we modify them, we remove them; and in each instance, we circumvent or attempt to circumvent the digital watermarks, which clearly are types of access or copy control technologies. When comparing different watermark systems or collecting data confirming that a watermark is defeated by a certain attack, it is not uncommon to engage in dozens to hundreds of separate acts of circumvention in a single day, each accomplished with a tool written for that very purpose.

20. Thus, the ramifications extend well beyond whether my colleagues and I can present a particular paper or publish a particular program. As much as we would like to publish tinywarp.c, doing so solves nothing if we are otherwise prevented from writing and using the tools that are at the core of our area of research.

21. Nor is it feasible to avoid the problem by seeking permission from the proprietor of a particular technology to attack that technology. First, seeking such permission is at odds with standard and well-accepted scientific practice. Scientists research that which they deem worthy of research, not just what third parties allow them to research. Second, it is unusual for a program written to attack one technology to not also have the ability to attack other technologies. We wrote tinywarp.c, for example, to attack SDMI Technology A. It did not accomplish what we wanted with respect to that technology, but a little experimentation revealed that it successfully attacked Technology F instead. It is highly likely that tinywarp.c, or perhaps a variant of it, would prove utile in attacking other digital watermarks.

22. We do not write and use programs such as tinywarp.c because we view breaking a

technology as an end unto itself. To the contrary, breaking a technology is nothing more than a crucial step either in attempting to improve the technology or in attempting to prove that the technology cannot be made to do what it is supposed to do. Both, of course, are legitimate research objectives, and in either case, writing and using tools to circumvent access or copy control technologies is essential to our work. If we can no longer use the necessary instruments of science, then our field of scientific work will be paralyzed.

23. The ability to determine if music, images or video clips contain hidden messages has important applications beyond mere copyright protection. There is an obvious application to law enforcement, for instance, as criminals may use information hiding techniques to conceal incriminating communication from authorities. However, because some companies also intend to use information hiding for copyright protection, legal hurdles prevent the development of techniques for finding hidden information.

24. In paragraphs 20 thru 26 of my first Declaration, I described a computer program I am writing as part of my dissertation. I have written most of the program's central infrastructure, the part that allows a user to open audio clips and set up statistical tests. I hope to have a functional but limited version of this program in the near future. I have made progress since my first Declaration, but it has been slow.

25. The purpose of this program is to provide others with tools and techniques for analyzing music, which might have hidden information (e.g., digital watermarks) embedded within. It is designed to allow a researcher to formulate various useful statistical tests, in search of clues and artifacts which can be found in music after information is hidden inside it.

26. Early in this program's development, I decided that it should not be able to alter, or remove, watermarks in music. The program would only be able to analyze, rather than alter, music files. This decision was motivated only by the DMCA, not by any inherent programming limitations or by what, divorced from the DMCA, I did or did not want to do with the program: I did not want to release a program which could be used to alter music in any way, because of the possibility that it could be used to circumvent copyright protection systems. The DMCA has had a direct effect on this program's overall architecture.

27. As I mentioned in paragraph 25 of my first Declaration, I am quite wary of inviting others to participate in the writing of this program, even though the complexity of it is such that it would be accepted practice in academia for others to help write it. The letter sent to Princeton by the RIAA was also sent to numerous other parties, including the employer of the program chair of the Information Hiding Workshop. This pressured the chair into withdrawing the paper, to avoid legal action. Another letter was sent to Xerox PARC, then employer of Drew Dean; Xerox took steps to suppress the paper.

28. This tactic, of applying legal threats to various parties (or their employers) was successful in compelling us to withdraw our paper from the Information Hiding Workshop, because too many people working for separate institutions were at risk of legal action. We could not guarantee everyone's safety in time for the paper's presentation date. Unless I have good reason to believe that my future research is not at risk of similar tactics, I have no choice but to take steps to avoid this scenario: I must not collaborate with people at other institutions, or people who could be harmed by litigation, forcing me to halt my work.

29. This is a concrete example of the chilling effect not only of the DMCA, but also of the

defendants' actions. My current research project is progressing slowly, does not benefit from the contributions of others, and will be artificially limited in certain ways, because of very realistic concerns about what may happen if I am not careful. This is not due to vague concerns of a hypothetical legal threat, but rather a result of witnessing a very real application of legal pressure against myself and my research group, earlier this year. This is not a baseless concern about a hypothetical threat of harm; it is a realistic concern about future threats, based on a previous threat of harm.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration is executed in Princeton, New Jersey on October 23, 2001.

_____

SCOTT CRAVER