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
Hon. Garrett E. Brown, Jr.
Case No. CV-01-2669 (GEB)
Civil Action

Declaration of Ross Anderson

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.

I, Ross John Anderson, of 10 Water End, Wrestlingworth, Sandy SG19 2HA, England, born 15/9/1956, do hereby make oath and say as follows:

1. I am Reader in Security Engineering at Cambridge University. This is a senior faculty post; I lead the security group at the University's Computer Laboratory. We are recognised as one of the leading research groups in the world in the field of information security.

2. I am a Fellow of the Institution of Electrical Engineers and also a Fellow of the Institute of Mathematics and its Applications. I hold the BA, MA and PhD degrees from the University of Cambridge.

3. My research focusses on security engineering – the art and science of building systems that remain dependable in the face of malice, error and mischance. I am the author of the textbook 'Security Engineering – A Guide to Building Dependable Distributed Systems' and about a hundred research papers on the topic. I am also responsible for teaching many of the practical aspects of computer science at Cambridge University, including courses on software engineering and electronic commerce, and organising group projects that teach students the difficulties of working in teams to tight deadlines.

4. Just as progress in civil engineering depends on understanding why bridges have fallen down, and in aeronautical engineering on the causes of plane crashes, so progress in security engineering depends on knowing how system protection mechanisms have, or could have, failed. It is well understood that we learn more from one system that fails than from a hunred systems from which no failure is reported. I have therefore conducted numerous surveys of security failure, in applications ranging from autoteller machines through prepayment utility meters to vehicle monitoring systems and pay-TV. These papers have become standard references in the industry, and have driven much of our group's research into more robust protection mechanisms.

5. The research we do is scientifically important, useful, legitimate and of benefit to mankind. I wrote the seminal paper on peer-to-peer systems ('The Eternity Service') which has since led many companies – from Microsoft down to small start-ups – to work on mechanisms for large-scale distributed data storage and retrieval, in which hundreds of millions of users may share the spare capacity on each others' hard disks for data backup. I coauthored the seminal paper on physical attacks on smartcards, which has led to a $2m EU research project to develop next generation smartcard processors – in which my team is a major player. I also coauthored the paper that introduced 'soft tempest' – the idea of reducing the compromising electromagnetic emanations from electronic equipment using software rather than hardware; this technique is already fielded in

the flagship email encryption product from Network Associates Inc. and has the potential to save the military forces of NATO countries over a billion dollars a year. Colleagues in my group coauthored the seminal papers on cryptographic protocols and on protocol verification.

6. Work I have done on copyright marking schemes is of particular relevance to this case. Copyright marking involves adding hidden information to a picture, an audio track, a video or some other work that is not perceptible to the normal user of the work but which, given knowledge of the correct keys, can be decoded to yield some information. This may be a copyright notice, in which case the mark is generally known as a watermark, or a serial number, in which case the mark is generally known as a fingerprint. This field of study had been of interest to us for some time, and suddenly became important in the mid-1990s. I organised the first international conference on it, the Information Hiding Workshop (IHW) in 1996.

7. At IHW 96, researchers from MIT proposed a method for marking audio in which they added an echo to the audio track at a level that was not perceptible to a human listener, but that could be detected using suitable signal processing techniques.

8. I coauthored the seminal paper on the vulnerabilities of copyright marking schemes, which appeared at the following IHW in Portland, Oregon, in 1998 ("Attacks on Copyright Marking Systems", with Fabien Petitcolas and Markus Kuhn, in the Proceedings of the Second International Workshop on Information Hiding, Portland, Apr 98, Springer LNCS vol 1525 pp 219–239). In that paper we demonstrated attacks on a number of first-generation marking schemes. Our attack on MIT's echo hiding technique was to use signal processing techniques to identify and remove the artifically added echo. Our work was not simply critical; it led to a tool (Stirmark) that is now the industry benchmark for testing marking systems.

9. I was therefore greatly surprised to learn that the SDMI consortium had adopted, as a critical part of its copy protection technology, the very echo hiding technique whose inadequacy we had previously demonstrated, and issued a public challenge to researchers to break their system.

10. I was much less surprised when, in my capacity as a member of the program committee preparing for the fourth IHW in Pittsburgh in April 2001, we received two papers showing how the SDMI challenge could be broken. Nonetheless, both papers were of a sufficiently high technical standard, and contained sufficient new material, that the committee decided to accept them.

11. The details of how an attempt was made by RIAA to suppress publication of one of these papers are told in the statement by my colleague John McHugh. I confirm the accuracy of his account insofar as it relates to me.

In particular, I attended the program committee meeting in the Wyndham Hotel, Pittsburgh, on the 24th April at which it was decided to offer the authors of the paper a speaking slot regardless of the threats uttered by RIAA. We felt it our duty to uphold the principle of academic freedom and the principle that it is a program committee's role to make technical judgments rather than legal ones. Nonetheless, this caused me some concern because of the potential personal liability issues. The professional indemnity insurance that we carry as University Teaching Officers does not cover the USA (as cover is too expensive), and having to defend a lawsuit in the USA (even a vexatious suit brought for tactical reasons and with no merits whatsoever) could be ruinously expensive. I understand that many other European academics are similarly exposed.

12. One of the other tasks that fell to the committee was to arrange a venue for the next IHW, in 2002. During the course of the conference, we received a number of informal bids, including one from Roger Dingledine of MIT to hold the next workshop in Boston. However, the action of RIAA, and the resulting threat of personal liability, had had such a chilling effect that I persuaded Roger not to develop his bid into a formal proposal. I pushed instead for the next IHW to be held outside the USA, in the hope that the legal situation would stabilise. As a result, we received only three formal proposals (from the UK, the Netherlands and Korea) and in due course decided that IHW 2002 will be held in Eindhoven in the Netherlands.

13. I am on sabbatical from September 2001 until October 2002, and my original plan had been to visit MIT, CMU and UC Berkeley for about six weeks each during this time. However, the continuing legal uncertainties about the DMCA have been a factor in my changing my plan so as to probably visit CMU and the National University of Singapore during 2001. My proposed visit to MIT may happen in 2002, or it may be replaced altogether by a visit to the Indian Institute of Technology in Madras. There have been further factors in this rearrangement, including another DMCA case (that of Dmitri Sklyarov) that has further exacerbated the chilling effect of the DMCA on international scientific collaboration; and the fact that CMU has offered me an adjunct post in which I will be covered by their third party liability insurance while MIT sought only to reimburse me through an existing inter-university arrangement (the Cambridge-MIT Institute) that would have left me as an employee of the University of Cambridge.

14. Security research at an internationally competitive level is inherently an adversarial business; the field advances through a coevolution of attack and defence. Understanding and documenting the vulnerabilities of existing systems is critical to progress. The prospect that I might be sued in the USA for research work done here at Cambridge University, and published in a responsible way through the usual academic channels, is alarming.

15. If a law-abiding serious researcher can face severe legal hazards because his work is seen as inconvenient or harmful by a large US company or consortium, then many of the top researchers in the field would be exposed to personal risk. For example, I have well known work on the security of smartcards, my research being conducted in partnership with the French company Gemplus and the Israeli company NDS. It poses a direct competitive threat to a US company, Atmel. If I publish an attack that breaks the Atmel product but not Gemplus's or NDS's product – even unwittingly – then it appears that Atmel might cause legal problems in the USA that would consume my time and my fortune. I am not an expert on US law, but this is certainly the impression that I have gained from this case. Rather than going to the expense of hiring US lawyers, it is simpler for me to avoid giving talks in the USA, or doing joint research in the USA, the subject matter of which might be covered by the DMCA.

16. I have for years been an opponent of the anti-Americanism that becomes fashionable in Europe from time to time, and that unfortunately reared its head again recently at Genoa. The Felten case does not help those of us who consider ourselves to be America's friends, and I seriously hope that the court may find some way to provide reassurance to the research community.

17. I believe that the contents of this statement are true.

Signed

Ross Anderson