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, | ) | Hon. Garrett E. Brown, Jr.<br>Case No. CV-01-2669 (GEB)<br>Civil Action |
| Plaintiffs, | ) | DECLARATION OF |
| vs. | ) | EDWARD LAZOWSKA |
| 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, EDWARD LAZOWSKA, of full age, hereby declare:

1. I am the Bill & Melinda Gates Chair in Computer Science in the Department of Computer Science & Engineering at the University of Washington, and a Member of the National Academy of Engineering. My *curriculum vitae* is attached as Exhibit A. I am a member of the Board of Directors of the Computing Research Association ("CRA") and served as its Chair for the past four years. I have been given authority to make the statements in this declaration not only personally, but also on behalf of CRA. I have personal knowledge of the facts set forth below. I submit this declaration to provide the Court with certain relevant facts regarding the chill cast over computing

research by the Digital Millennium Copyright Act, and more particularly, by the threats and actions of the defendants in the matter before this court.

2. CRA is an association of approximately 200 North American organizations active in computing research. These organizations include academic departments of computer science and computer engineering; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies. A listing of CRA members is attached as Exhibit B.

3. CRA works with its member organizations to strengthen research and advanced education in computing and allied fields. CRA takes very seriously the "research" in its name. Thus we are particularly concerned that the anticircumvention provisions of the Digital Millennium Copyright Act ("DMCA") inhibit computing research or dissuade computing researchers from pursuing an entire class of problems.

**The nature of computer systems research**

4. Much research in computer systems is based upon *analysis* – the careful examination of existing systems and approaches in order to understand what works well and what works poorly. This sort of examination leads to improvements that are both evolutionary and revolutionary. Researchers discover flaws. They invent new and improved ways to detect and correct flaws, and they invent new and improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward at an extraordinary pace for more than half a century.

5. Analysis is no less important when the system being studied is used to protect copyrighted works. Indeed, because the same basic elements used in copyright- and access-protection systems may be used in systems to protect the privacy of personal communications, the confidentiality of business data, or the security of financial transactions, to name a few, there is no bright line between study of systems with different practical applications.

6. The best encryption systems are not one-off systems designed from scratch for single use, but designs that build upon prior research. For this reason, it is critical that the researchers and engineers developing new systems be able to study existing ones for advantages and flaws. In turn, a system's ability to withstand repeated attacks best allows engineers and the public to trust its security.

**The importance of open discussion and publication to computing research**

7. Open discussion of computing research and publication of its results is essential to the conduct of computing research. The computing research community is large – many thousands of individuals. It is ever-expanding: students join the research community and mature researchers move from one sub-field to another, in each case by studying the literature, just as in almost every other area of study. In computer science research, the "literature" includes code, algorithms, and their analysis.

8. Broad review and critique are fundamental to the advancement of research. Many computing research journals employ a peer-review process to select and refine papers for publication. The essence of peer-review is critique from "outsiders" not involved with the paper's underlying research, and the process depends upon the new perspectives reviewers bring from *not* being collaborators in a paper's development. Like other scientists and medical researchers, computing researchers use peer review to subject their claims to independent verification.

9. All of computer science, and indeed all of science, is increasingly interdependent – results in one field or sub-field are relevant to researchers in other fields or sub-fields. Closed communities do not make progress at nearly the rate of open communities. For these reasons, CRA works to bring together diverse parts of the computing research field, to strengthen research efforts by bringing cohesiveness to the professional community. It does this in part by sponsoring interdisciplinary conferences and encouraging researchers to publish and discuss their work with those outside their research niche.

10. Every three years, for example, CRA co-sponsors the Federated Computing Research Conference, a conference that brings numerous specialized computing research meetings and conferences together at the same time and place, enabling cross-communication among researchers who are not ordinarily in collaboration.

11. There is a long history of open research in computer security and information hiding. This is obvious simply from the fact that the Felten *et al*. paper was submitted to the *Fourth* International Information Hiding Workshop and then to the *10th* USENIX Security Symposium. Most of the security and information hiding technologies upon which we rely today are the products of this open research process.

12. The Felten *et al*. paper provides a useful case study of this research process, and of the benefits of open publication. For those who do research in copy protection or information hiding, the paper provides a careful scientific case study of six approaches, using a variety of analytic techniques. The paper makes specific contributions to deepening our understanding of why watermarking based upon echo hiding is not a viable technique – a fact first exposed in a paper published two years earlier

by R. J. Anderson and F. A. P. Petitcolas (On the Limits of Steganography, *IEEE Journal of Selected Areas in Communications 16*,4 (May 1998)). The Felten *et al.* paper exposes the hurdles that future watermarking techniques must overcome if they are to be successful. The paper has *already* led to significantly improved approaches to watermarking.

13. For those who are indirectly interested in copy protection or information hiding – for example, potential users rather than researchers – the paper demonstrates that the approaches advocated by RIAA, SDMI, and Verance will not provide protection. This information is important, for example, to recording studios or recording artists considering these technologies for protection of their work. Indeed, there is a market for copy protection schemes in which these watermark schemes (and the companies which develop them) compete. With free flow of information about the cost and quality of different copy protection schemes, this market should lead to the production of better and cheaper schemes. By chilling the flow of information about the quality of competing copy protection schemes, the DMCA cripples the market's ability to reward higher quality schemes.

14. More generally, computing history is filled with examples of developments that drew upon cross-fertilization among disciplines, often unexpectedly. The RSA cryptography system that now underlies many secure communications was developed by complexity theorists (a field at the interface of mathematics and computer science) Ron Rivest, Adi Shamir, and Len Adelman after they learned of and applied their expertise to the public key cryptography work of Whitfield Diffie and Martin Hellman.

15. Breakthroughs in the theory of graph coloring algorithms from the theoretical computing community were later employed by the compiler community to optimize register allocation. That in turn enabled computer architects to design computers with more registers, a breakthrough that spawned the

faster Reduced Instruction Set Computers (RISC) that have been in widespread use since 1985. (*Computer Architecture: A Quantitative Approach, 2nd Edition*, Hennessy and Patterson, 1996, at 92).

16. Computer anti-virus experts rely heavily on public dissemination of timely information about threats on the horizon. For instance, the recent "Code Red" worm was designed to spread rapidly for about a week, and it was very successful at infecting more than 200,000 computers. Security researchers across the country rallied together in a concerted effort to blunt the attack, and discovered through last-minute reverse engineering (disassembly) that the worm was designed to make all infected machines attack the White House web server on a specified date. With only a few days to counter this threat, experts were able to study the reverse engineered worm to identify a weakness of the attack and counter it, protecting the White House web server and others. This containment of the Code Red worm would not have been possible without immediate, unrestricted public dissemination of full information about its spread, which included open discussion of the flaws it exposed in other computer software.

17. In 1989 complexity theorists Adi Shamir and Eli Biham invented the technique called differential cryptanalysis, which called into question the strength of the famous DES block cipher, which was then being used by all commercial banking systems and by the U.S. government. Nonetheless, the two scientists were treated as heroes rather than criminals. Their invention of differential cryptanalysis taught the encryption community how to design block ciphers to resist this class of attacks. In fact, the newly adopted AES block cipher (the Federal Advanced Encryption Standard adopted by the U.S. Government) is specifically designed to resist differential cryptanalysis. In other words, the publication

of a new means of attacking encryption — differential cryptanalysis — made it possible for the research community to design the AES block cipher that is now the federal encryption standard. The analogy to watermarking is obvious. A break of a watermarking system teaches the research community how to design better systems. If a break exists it will be discovered. It is much better from everyone's perspective if researchers discover the break and publish it than if unscrupulous discoverers of the break exploit it without public notice.

18. The DMCA, however, chills research and publication when the technologies or systems in question are used to protect copyrighted works. It effectively allows copyright holders or the manufacturers of copy- and access-control technologies to preempt a field of research simply by choosing to encrypt copyrighted works with the technology. Even the statutory exceptions force researchers to justify their efforts to copyright holders before they begin work.

**The chilling effect of the DMCA's anticircumvention provisions**

19. CRA is concerned that as written and as invoked by the RIAA, SDMI, and Verance, section 1201 of the DMCA has a substantial chilling effect on computing research. Fears of violating vaguely-defined prohibitions are expected to lead researchers to choose "safer" topics of study than encryption and data-hiding and to censor their publications rather than risk lawsuits.

20. While computing researchers do not intend to violate copyright law, this law is unclear on what exchanges of information might be deemed to "offer to the public, provide, or otherwise traffic in [a] technology, product, service, device, component, or part thereof" that is subject to its prohibition, as primarily designed for circumvention or having limited non-circumvention commercially significant

purpose or use. The ambiguity of the law may lead researchers to steer a wide berth away from encryption and data-hiding research that relates to access- and copy-control schemes.

21. Since in computer science as in other academic disciplines, publication is important to advancement in the field, students are less likely to choose areas in which they fear they will be unable to publish their results, and professors will hesitate to recommend these fields so strongly. As a result, less research and investigation is likely to be done in encryption and data-hiding fields chilled by the DMCA.

22. In particular, the DMCA's references to "technology," including a "component or part thereof" of a circumvention technology could be read to encompass the snippet of code a researcher includes in his paper as part of his explanation of a newly-discovered security flaw. SDMI, in threatening Felten *et al.* with suit over the publication of their research paper, appears to take this broad view, including research papers within the ambit of prohibited "technology."

23. The prong of the anti-device tests that captures technologies with "only limited commercially significant purpose or use other than to circumvent" may likewise fail to shield researchers — whose intermediate-stage work may have *no commercial* purpose. The commercial significance of much theoretical computing research is realized only long after its initial publication. For example, in 1988, British mathematician John Pollard invented a new factoring algorithm, the number field sieve. Last year, in 2000, this algorithm was used to break the RSA-512 challenge, showing important insecurities in 512-bit RSA keys, and prompting the industry to institute 1024-bit keys in their place. Only the publication of Pollard's research and its use when it had no "commercially significant purpose" allowed researchers to follow it up with improvements to computer systems in commercial use.

24. As described above, collaboration in computing research often arises serendipitously, when one researcher's interest is sparked by a detail in a paper on a topic far removed from his or her own. These researchers may end up "working collaboratively" only because they were able to meet through the sharing of information. Yet the DMCA chills the publication of just the details that might interest one researcher in another's work — unless the permission to share decryption technology among those "working collaboratively" extends to the wide range of potential collaborators.

25. From my perspective, as an active computing researcher and one who directs and collaborates with others on research, the exceptions of 1201(f) and (g) do not reach far enough to protect computing research as it is actually done. For example, 1201(g) purports to exempt activities "necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works," yet the exception places burdensome pre-conditions on that research, unreasonably limits who may perform it, and stifles publication of its results.

26. The DMCA fosters a dangerous information imbalance. In this case, for example, it allows the publishers of encryption technology to claim greater efficacy and security than their products warrant, then use the law to silence those who would reveal the technologies' flaws. In this case, the law gives content providers a false sense of security, achieved through law, not technical effectiveness. Preventing researchers from discussing a technology's vulnerabilities does not make them go away — in fact, it may exacerbate them as more people and institutions use and come to rely upon the illusory protection. Yet the commercial purveyors of such technologies often do not want truthful discussions of their products' flaws, and will likely withhold the prior approval or deny researchers access for testing if the law supports that effort.

27. The recent arrest of a Russian researcher has only added to CRA members' concerns about the breadth with which the DMCA is being applied. Dmitry Sklyarov, a Russian Ph.D. student, was in the country for a computer security conference at which he gave a presentation on the insecurity of Adobe's eBook encryption technology. Following the presentation, he was arrested and charged with trafficking in a product designed to circumvent copyright protection, in criminal violation of the DMCA, based on his employer's sale of a software program to read encrypted eBooks. (Criminal Complaint, July 17, 2001 <http://www.usaondca.com/press/assets/applets/2001_07_17_sklyarov.pdf>) Since that arrest, CRA members have heard from several foreign researchers who are now planning to curtail visits to the United States — including attendance at computing research conferences — because they fear their research might make them targets of similar lawsuits or prosecutions. Alan Cox, a prominent British Linux kernel programmer, resigned from a USENIX committee, saying that he felt it was no longer safe for foreign software engineers to visit the United States.

28. CRA is vitally concerned that the pall cast by the DMCA's anticircumvention provisions will stifle its members' research efforts and weaken academic computing research programs. In turn, we fear the shadow of the law's ambiguities will reduce our ability to contribute to industrial research in encryption and data-hiding technologies at the heart of our information infrastructure.

29. I declare under penalty of perjury that the foregoing is true and correct. Executed on August 9, 2001, in Seattle, Washington.

Dated: August 9, 2001

_____
Edward Lazowska


_____
Grayson Barber (GB 0034)
Grayson Barber L.L.C.
68 Locust Lane
Princeton, NJ 08540
phone (609) 921-0391
fax (609) 921-7405

Gino J. Scarselli
664 Allison Drive
Richmond Hts., OH 44143
(216) 291-8601 (phone and fax)

Cindy A. Cohn
Lee Tien
Robin D. Gross
Electronic Frontier Foundation
454 Shotwell St.
San Francisco, CA 94110
phone (415) 436-9333
fax (415) 436-9993

_____
Frank L. Corrado (FLC 9895)
Rossi, Barry, Corrado & Grassi, PC
2700 Pacific Avenue,
Wildwood, NJ 08260
phone (609) 729-1333
fax (609) 522-4927

James S. Tyre
10736 Jefferson Blvd., # 512
Culver City, CA 90230-4969
phone (310) 839-4114
fax (310) 839-4602

Joseph P. Liu
Boston College Law School
885 Centre Street
Newton, MA 02459
phone (617) 552-8550

Attorneys for Plaintiffs

**EXHIBIT A**
**Curriculum vitae of Edward Lazowska**

**EXHIBIT B**
**Membership list of the Computing Research Association**