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,

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

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,

DAVID WAGNER

Defendants.

I, DAVID WAGNER, of full age hereby declare:

I am an Assistant Professor of Computer Science at the University of California,
Berkeley. I received an AB in Mathematics from Princeton University in 1995, a MS in
Computer Science from Berkeley in 1999, and a PhD in Computer Science from
Berkeley in 2000. I am personally familiar with the facts set forth herein, and if called as
a witness, I could and would testify thereto of my own personal knowledge.

2. My area of research includes computer and telecommunications security, cryptography, privacy, anonymity, and electronic commerce. Cryptography is the science of designing and analyzing secure codes and ciphers.

3. I have published extensively on the subjects of cryptography and the security of computer systems. A list of my publications is included in my C.V., attached hereto as Exhibit A.

4. I also teach "Security in Computer Systems" at Berkeley, a graduate-level course on modern computer and network security.

5. My work (I have done data security consulting through Counterpane Systems, Minneapolis, and independently), my studies (in addition to my work at Princeton and Berkeley, I twice interned at Bell Labs, studying under S. Bellovin) and my teaching have given me extensive experience in the analysis of real-world security systems. The systems I have personally examined include supposedly secure systems used by hundreds of millions of people. Many of my discoveries have resulted not only in academic publications, but also in widespread news coverage in leading newspapers, magazines, and TV news shows. For example, in September 1995, a colleague and I reported serious security flaws in the techniques used for encrypting credit card numbers in the leading products facilitating the implementation of electronic commerce over the Internet. This discovery was reported on the front page of the New York Times, the front page of the business section of the Washington Post, and elsewhere.

6. In March 1997, two colleagues and I reported on flaws in the privacy codes used by U.S. digital cellular phones, phones used by tens of millions of U.S. citizens. This work not only received widespread news coverage (e.g., the front page of the New York Times), but also helped convince the U.S. cellular standard committee to undertake a sweeping re-design of their security architecture.

7. In April 1998, two colleagues and I reported on weaknesses in the privacy and billingsecurity protections found in GSM digital cellular phones. GSM is the European cellular telephony standard, with over two hundred million users worldwide. Again, this work received widespread coverage in leading newspapers such as the front page of the business section of the New York Times, page A3 of the Wall Street Journal, and other similar locations.

COMMUNICATION IS CENTRAL TO CRYPTOGRAPHY

8. Cryptography is the study of how to communicate securely. Interest in cryptography has dramatically increased in the past few decades, and there is a broad research community actively working to advance scientific knowledge in this area.

9. Scientific research into cryptography is at its heart a collaborative process involving the entire research community, and as such is organized around many forms of communication between researchers. Communication is of course central to most scientific fields, but unfettered communication is especially crucial to scientific progress in encryption technology because of two unusual properties of the field.

10. First, the process of gaining confidence in an encryption technology is fundamentally a community-oriented process. Experience shows that many encryption systems have unexpected flaws when initially proposed. The response of the scientific community has been to place a very high value on careful analysis of proposals by many researchers. It is easy for one researcher to overlook subtle flaws, but what one researcher overlooks another might discover. Designing secure encryption technology is possible but costly: historically many candidates have been found to contain subtle defects, and so the design task requires dedicated effort by the entire community. As a consequence, years of intensive public scrutiny are often required before a new encryption technology becomes accepted by the scientific community.

11. This system of careful and public scrutiny of new encryption techniques has been very effective at improving the quality of encryption systems used around the world.

However, it rests on a bedrock of communication at all stages in the process. The first step is formal publication of the cryptographic technology in the scientific literature, after some level of peer review. Then, the community has a chance to gain confidence in the system as other researchers publish the results of their analysis of it in the literature.

12. Second, in cryptography the study of code making and the study of code breaking are inseparably intertwined: to be a good code maker, one must have a deep understanding of code breaking. One must think like an adversary in order to anticipate how one's own encryption system might be attacked.

13. Because cryptography is fundamentally an adversarial science, we must anticipate all the possible clever ways that an adversary might try to break our security measures. In many settings, potential adversaries may have strong incentives to attack our security system, and the adversary may be able to muster considerable technical and financial resources. Once an encryption system is deployed, it may remain in place for decades before it is replaced. As a consequence, it is critical to anticipate in advance the way the encryption system could fail, to uncover flawed systems before they are widely deployed.

14. The branch of the science of cryptography which focuses on discovering or inventing ways that encryption systems may fail is called cryptanalysis (code breaking). The cryptographic community has devoted considerable attention to this area, and as a result many fundamental scientific advances in cryptanalysis have been made in the past

three decades. Cryptanalysis techniques are regularly applied to encryption systems that we ourselves have invented, as well as those invented by others.

15. Progress in cryptanalysis is crucial for progress in the design of secure cryptographic systems. The known cryptanalytic techniques are used as a benchmark to evaluate potential designs, and this gives us a way to quantify their strength against attack. Review of proposed encryption technologies is critical to further progress in understanding how to build secure computing systems.

16. These two properties of cryptography (community-oriented processes, and the importance of cryptanalysis) make communication important to the progress in field.

17. Communication in this field takes many forms. Roughly speaking, there seem to be two major ways that cryptographers communicate: through informal venues, and through formal publication in the literature.

18. Formal publication follows a scripted process designed to ensure a certain level of quality. There are several classes of venues for formal publication, including, for example, journals, conferences, and workshops. At each, a committee or editorial board of respected researchers reviews submissions according to their technical merit and typically accepts a small number of submissions. Accepted journal papers appear in the journal's proceedings; many journals and conferences also publish their proceedings online on the World Wide Web (over the Internet). Accepted conference and workshop

papers generally appear in the published proceedings of the conference as well as being presented in person at the meeting of the conference with a talk given to the attendees.

19. The literature, which is made up of all formally published papers, is central to the scientific field. It defines the known state of the art, and almost all advances appear in the literature. Formal publication is one of the main ways that cryptographers communicate about the results of their work to the world. It should be no surprise that the productivity of academic and other scientific researchers is often measured by the papers that they publish.

20. Because formal publication is reserved for reporting on results of research that is at least partially completed and of high quality, researchers also communicate through many informal means. Informal communication often takes place early in the research process, before formal publication. Informal conversations may be held in person (at academic, technical, or other scientific conferences, meetings, and in hallways), over the phone, or over the Internet. Many institutions hold talk seminars where researchers give informal talks on their current work. Work-in-progress sessions at conferences and workshops play similar roles. In addition, researchers often share paper drafts, algorithms, computer programs, and other material on paper or over the Internet, either privately or publicly. Some researchers also regularly make their papers available to the public before they are published, and this is done in many ways: they can be made available over the Internet, submitted to an organized pre-print service (designed exactly for this form of rapid communication), or issued as a technical report (which means that

the hosting institution makes them available to the public, sometimes for a nominal copying fee). These forms of private and public communication allow researchers to bounce half-formed ideas off colleagues, find potential collaborators, discuss progress with co-workers, obtain comments from others in the field, and communicate results to the greater scientific community.

21. Because the cryptographic field moves so rapidly, informal channels of communication are necessarily widely used. Conference publication typically involves delays of 6 months to a year, and journal publication has even longer delays. By this time, industry may have made decisions without the benefit of this knowledge. As a result, many scientific papers are made available to the public (often on the Internet) in advance of formal publication.

22. The Internet recently has acquired special significance for research because it allows researchers to make their work available to other researchers and to the public inexpensively, easily, and rapidly. For example, I routinely make every paper that I write available over the Internet (on my web site) as soon as it is finalized and accepted for publication, which is usually months in advance of the date of formal publication. Many other researchers do so as well.

COMMUNICATION TAKES MANY FORMS

23. Communication between cryptographers routinely involves much more than mere text. Cryptographers also rely heavily on mathematics, algorithms, source code, and executable programs for communication. The reason is partly due to a recent trend in cryptography.

24. Over the past several decades, the field of cryptography has been revolutionized by the widespread availability of computers. In the past, encryption was often done by hand, but this limited the complexity of any such process to the level of what a human could perform manually. Computers make it practical to routinely use much more sophisticated forms of encryption at vastly reduced cost, and as a consequence the study of cryptography today focuses primarily on encoding processes that can be automated by computer.

25. In computer science, a computational process is often described by presenting an algorithm. An algorithm is an abstract mathematical specification of a process for performing some computational task (roughly analogous to a "recipe" in cooking). Algorithms often serve as both descriptive communication as well as a template for implementors.

26. Programmers build a concrete implementation of an algorithm by expressing it as source code for some programming language. A programming language is a stylized and precise notation for specifying and communicating precisely how a computational task is to be performed and for describing the programmer's assumptions and intentions.

27. There are many programming languages. High-level languages often focus primarily on specifying the goals of the computation, leaving the compiler free to choose some aspects of how to achieve those goals. Low-level languages specify in great detail each of the steps of the computation, with no ambiguity. Others fall in between. High-level languages are usually compiled (translated) down to a lower-level language, rather than being executed directly. Several steps of compilation may be used: for example, C source code (a medium-level language) is compiled to assembly language (a low-level language), which is compiled to executable object code (a set of instructions ready for direct execution on a computer).

28. Most programmers find it easier to understand and develop code expressed in high-level languages (which are designed to be convenient for people) than in low-level languages (designed to be convenient for machines). However, trained programmers can and do read and write code at each of these levels. Computer scientists frequently use each of these forms of expression to communicate ideas, choosing whichever form of expression communicates the idea most clearly. Just as mathematicians freely mix both mathematical equations and English text, so too do computer scientists use equations, algorithms, code, programs, and text as tools of communication.

29. Algorithms are often described in what is known as "pseudo-code", which conveys the ideas in a similar style to source code (but pseudo-code is not necessarily executable on any machine). Other times, algorithms are described by giving a source

code implementation. Showing an algorithm in pseudo-code is often an extremely concise way to describe the structure of computation while abstracting away some of the straightforward but distracting implementation details, while source code gives a more precise description of all details of the computation, leaving less up to the imagination.

30. For example, many papers in the cryptographic literature start by presenting the encryption algorithm that is being proposed or studied in the paper, and may show many algorithms throughout the text of the paper. It is not unusual to find that a paper proposing a new encryption algorithm gives a source code implementation of the algorithm in the body of the paper. This allows a very precise specification of the behavior of the algorithm, so there can be no confusion.

31. Although I have categorized these forms of communications into several distinct clusters, in practice there is no clear distinction between these different forms of communication. Rather, there is a smooth spectrum of forms of expression---- encompassing pictures, mathematical equations, algorithms, pseudo code, source code, object code, and executable programs---that allows the writer to trade off precision against conciseness and other qualities. The choice of a form of communication is typically based on pragmatic concerns for how to communicate the intended idea most efficiently. In general, computer science is concerned with the study of functional objects, and these forms of communication provide a uniquely concise and effective way to describe the relevant aspects of these functional objects.

PRECISION IN COMMUNICATION IS OFTEN A PREREQUISITE FOR PROGRESS

32. The cryptographic properties of an encryption algorithm can depend critically on the exact details of the algorithm. Some approaches to encryption are weak no matter how you fill in details, but in most cases, the details matter greatly. Often a slight change in an encryption algorithm can dramatically affect its security: changing a few small details can change a secure algorithm to one that is easily broken. As a result, thorough analysis of any encryption algorithm often requires an opportunity to understand precisely what the algorithm is.

33. In addition, absence of ambiguity is especially crucial whenever an algorithm is intended to be implemented on a computer, because computers do not tolerate ambiguity. These two motivations explain the meticulous care with which proposed encryption algorithms are typically described in the scientific literature.

34. For these reasons, cryptographers rely on ability to communicate precisely. Cryptographers would be handicapped without the ability to utilize these precise and efficient modes of communication.

IN COMPUTER SCIENCE, PRECISION OFTEN REQUIRES COMMUNICATION OF CODE

35. To achieve this level of precision, computer scientists use algorithms, equations, and code (among other tools) in their communications. These various forms of expression are not interchangeable, and code is especially valuable where maximum precision is required. In some cases, there is no other way to communicate as clearly, concisely, and effectively as is possible with source or object code.

36. Computer code is expressive. Computer code is often also functional, in the sense that it can assist a person to perform some function or activity. Strictly speaking, not all code is functional: for instance, pseudocode is not directly executable, and is solely an abstract description of a functional object. However, in general, precision and functionality go hand in hand. Because computers do not tolerate ambiguity well, source code is necessarily very precise, and many ways of expressing ideas in computer science (such as source code) are unambiguous exactly because they describe the idea in enough detail to enable execution on a computer. This means that code is a valued form of communication precisely because it is partly functional.

37. For these reasons, communication of source and object code play an important role in progress in computer science. This role is heightened further in cryptography, where precision is of extra importance.

REVERSE ENGINEERING PLAYS AN IMPORTANT ROLE IN CRYPTOGRAPHY

38. Researchers also rely on inspection and communication of executable object code from time to time. Although for many purposes source code in some high-level language is preferred to object code for communication (because it is more convenient to understand), source code is not always available. When all that is available is an executable program, one standard way to understand what the program is doing is through reverse engineering.

39. Many computer systems available on the mass market are available only in executable code, which contains a set of instructions for the computer to follow, specified in a low-level language designed to be convenient for a computer to process, but not especially convenient for humans to understand. The contents of these instructions are readily available, but their meaning may not be readily apparent to those untrained in the field. Reverse engineering such a system requires one to comprehend the computer instructions and translate them into a simplified form that others can understand.

40. The reverse engineer studies a product in depth and, by translating an obscure, machine-oriented language into plain English, is able to summarize the product's relevant features in a more comprehensible and useful form. Reverse engineering is often tedious and time-consuming because computer programs are extremely verbose (by human standards), but it is not in principle difficult.

41. There are many ways to reverse engineer a program. In principle, the simplest way is to read the object code directly; in practice, this approach is almost never used,

though, because although it possible to read and understand object code, doing so is not especially convenient for humans to understand. To ease the task, most programmers use a disassembler, a tool that automatically reverse-translates the object code into assembly language. More sophisticated tools are also available: for instance, it is frequently useful to reverse-compile the executable to obtain an approximation of the original source code and use that to understand the program. There are other techniques for reverse engineering as well. At present, reverse engineering is tedious and time-consuming, so it is typically used only where necessary, but for some tasks it is irreplaceable.

42. Reverse engineering is an accepted practice in computer science. Disassemblers and debuggers are regularly used by programmers in all fields of computing for understanding what a program is doing and for repairing programs that aren't working correctly. Indeed, a standard part of most undergraduate educations in computer science involves learning how to use a debugger and a disassembler, and how to read and write assembly language.

43. Based upon my experience and participation in and my observation of the academic and research communities at the University of California, Berkeley, I believe that reverse engineering is necessary, standard, and good for software and consumer electronic products containing encryption or other security features. Many of these products are available only in object code form, and as a result independent product reviews of such products would in many cases be impossible without the aid of reverse engineering. Independent reviews have proven essential for dependable security in the

encryption industry; they help consumers make informed purchasing decisions, and they enable and motivate innovation in improved security systems.

44. Researchers in the academic community often provide essential evaluations of cryptographic and other security measures used to protect our information infrastructure. Their work is particularly valuable because they have no financial interest in the outcome of these evaluations and because manufacturers do not always have the incentive or talent to undertake thorough examinations themselves. Publication and circulation of results of such evaluations is an accepted way to share ideas and advance scientific knowledge about cryptography. These applications of reverse engineering are, of course, motivated not by financial or commercial gain, but rather by scholarly progress and by a desire to do research in the public benefit, and reverse engineering is often the enabler that allows academics to do this research.

45. A number of my practical contributions to security and cryptography have relied on reverse engineering. In 1995, a colleague and I discovered that electronic commerce was potentially at risk because of a flaw in the encryption that was implemented in the popular Netscape web browser; because we warned the manufacturer, they were able fix the flaw before serious harm was caused. We found this flaw only after disassembling the product, and our discovery partially helped to motivate a widespread movement to take security very seriously in electronic commerce applications. In this case, we spent several days reverse engineering the implementation, and once we understood how it worked it took only a few minutes to discover the presence of a flaw. This experience is not uncommon: once the algorithm is revealed (e.g., through reverse engineering), it is often easy to check for flaws, but it might take years before someone bothers to reverse engineer the algorithm and publish it.

46. In 1998, colleagues and I discovered flaws in the security of cell phones used by 50 million people worldwide: by reverse engineering the proprietary, unpublished cryptographic algorithms used in these cell phones, we were able to show that various defects allowed the possibility of billing fraud.

47. Later in 1999, through further reverse engineering efforts we uncovered serious privacy vulnerabilities in these cell phones as well. Since then, our revelation of these previously unpublished algorithms has enabled further progress in the evaluation of cell phone security: we are aware of several follow-on publications in the literature, and one even led to fundamental advances in the theory of stream cipher cryptanalysis. (This is not unusual: examining real-world systems sometimes raises questions that can lead to fundamental improvements in our understanding of the field.)

48. These are just a few of the more prominent cases where my research has involved reverse engineering. None of these discoveries would have been possible without the ability to reverse engineer, and none of these uses of reverse engineering were motivated by interoperability or by profit.

49. For these reasons, reverse engineering (for reasons other than interoperability or commercial gain) is of special importance to the fields of computer security and cryptography, with impact both on fundamental research as well as on real-world practice.

NON-TRADITIONAL SPEAKERS ENABLE PROGRESS IN CRYPTOGRAPHY

50. Cryptography and computer security is not a closed community. Many important contributions have been made by people who are not engaged in a legitimate course of study, employed, trained, or experienced in the field of cryptography.

51. I have benefited from non-traditional contributors many times in my own personal experience. My early work discovering flaws in the Netscape web browser was undertaken less than a month after starting as a first-year graduate student, with little experience and no credentials. Later, when I examined GSM security cell phone in 1998, I undertook this project in collaboration with Marc Briceno, a privacy enthusiast with no academic credentials in the field of cryptography. This research would not have happened without Briceno's assistance: reverse engineering the GSM security algorithms was a prerequisite for studying them, and as graduate students with many responsibilities, we did not have time to spend the many months needed to accomplish this reverse engineering; Briceno did.

52. There are many other examples. Flaws in DVD security were found only after an unknown party reverse engineered and revealed the DVD algorithm; a few days later, serious flaws were found by an interested party who was not previously known in the cryptographic research community. Flaws in HDCP, the High-bandwidth Digital Content Protection standard, were recently found by another interested party without credentials in the cryptographic research community. These cases illustrate that newcomers to the field routinely make important research contributions.

53. Part of the importance of outsiders to practical security research is due to the need for reverse engineering. In many cases, reverse engineering is required before a commercial system can be analyzed. Unfortunately, reverse engineering is time-consuming, tedious, and uninteresting to most academics. Reverse engineering is usually not considered research---it is too straightforward for the process itself to be considered novel research---and so it is hard for a credentialed, experienced academic to justify spending time on reverse engineering. Without uncredentialed outsiders, the reverse engineering that is a prerequisite for research into the security of real-world systems might never become available.

54. Fortunately for cryptographers, any trained or experienced individual anywhere in the world can reverse engineer a computer software product; this work is not restricted to engineers, professionals, industry professionals, or graduate students. As a result, scientists often rely on non-traditional speakers, and many valuable research contributions can be directly attributed to the presence of outsiders and amateurs. Individuals who lack high academic credentials and even "regular" jobs have contributed to some very important results and have advanced the science significantly. Marginalizing these individuals would be a loss for the field and could stifle scientific progress.

THE DMCA HAS CHILLED MY OWN SCIENTIFIC ACTIVITIES AND HAS LED ME TO ABANDON MY RESEARCH IN COPY PROTECTION

55. Concerns about the DMCA have directly affected my current research and have led me to conclude that I can no longer conduct scientific research in the area of copy protection. Specifically, this conclusion arose from my recent experience on HDCP, a copy protection system designed for controlling digital video communications. HDCP does not seem to be widely used today. However, reports indicate that HDCP will likely to be deployed in conjunction with digital TV products in the near future, and I expect it will be found in products used by millions of consumers. As discussed earlier, once systems like this become widely deployed, it is too late to fix any flaws that may be found. My interest in HDCP stems partially from the observation that we have a unique opportunity in this case to identify and fix any flaws in HDCP before it is too late.

56. The publication of the HDCP specification was brought to my attention in early May 2001, and on May 24, I sent a note to five colleagues suggesting that this might be worth our attention. One of these was a student of mine; three were other students at Berkeley who I had worked with before; and the fifth was someone with whom I have collaborated

closely for many years. This was a normal and routine thing to do, as copy protection is a field of considerable scientific interest. After my suggestion to look at HDCP, an email discussion ensued, and by 8:00pm the same evening, our investigation had revealed that HDCP had serious security weaknesses. Our goal was to understand and describe these weaknesses.

57. Later we discovered that another researcher, Scott Crosby, had independently come to a similar conclusion in his research. It seemed clear that little scientific purpose would be served by publishing the same results in two separate papers, and so, as is common in this situation, we mutually agreed to collaborate in preparing a joint paper.

58. Then in June 2001, we found that a researcher in the Netherlands, Niels Ferguson, had examined the security of HDCP and even found serious risks that went beyond anything we had found. We subsequently invited him to join us as well. I have collaborated with Niels many times before, so I knew he would have important contributions to make and I hoped he would agree.

59. Sadly, Niels eventually declined, mentioning concerns about the DMCA's impact on collaborating with US citizens. I consider this a loss for us, and for the science.

60. Ferguson's unpublished manuscript makes several scientific contributions above and beyond our paper, and as a result of Ferguson's subsequent decision not to publish due to DMCA concerns, it is not clear whether these observations will ever be revealed. In addition, I'm concerned by signs that the chilling effects of the DMCA are already making it harder for those of us in the US to collaborate on research with foreigners.

61. The DMCA also was the basis for us to censor ourselves in our presentation of our work on HDCP. We were at first unaware of the legal pitfalls. Then we attended the Usenix Security conference, where on August 15, Craver et al. presented their paper on SDMI (sometimes known as "the Felten paper"). We realized that the DMCA could pose a serious risk for us, much as it did for the Felten group, since our research, as Felten's, required the description of methods of circumvention of HDCP security. As Rob Johnson, a Ph.D. student working with me, was scheduled to present a short talk on our HDCP work at a work-in-progress two days later, we hastily sought out legal advice.

62. Johnson did give a talk on our work two days later, on August 17, but due to the legal risks, we decided to self-censor our talk. The version of the talk we had planned to give included technical details on the security weaknesses we had found in HDCP, but at the last minute we decided to delete that information: due to the legal risk, we felt compelled to limit our talk to information that was already publicly available along with a brief statement (without elaboration) that we had found weaknesses in HDCP. This change was not in the best interests of the field, but we felt it was necessary to protect ourselves.

63. After returning from the conference, I contacted UC Berkeley's Assistant Chancellor of Legal Affairs, Michael Smith, for legal advice. After some study, Smith advised us

that we were at risk for civil liability under the DMCA if we published. He stated that he could not predict whether we would win a lawsuit if sued. Smith also warned us that the encryption research and other exemptions of the DMCA would be useless to us if we were sued under Section 1201(b). I contacted several other lawyers for independent advice, and they concurred with Smith's assessment.

64. At the end of the day, we have been left with a clear conclusion that the law was not clear enough for us to determine whether we could publish our work without danger of being sued. We were also informed that the potential liability exceeded the sum of our personal assets and that the litigation itself could be extremely expensive. This, plus the experience of the threats made to Professor Felten's research team leaves us (and our legal counsel) unable to assess how likely it is that we will be sued or that the suit will be successful, but with a clear picture of the dire consequences if we are. To say the least, we are taking these legal risks very seriously.

65. I believe that publication is in the best interests of the field, so I will continue to follow all avenues available to us. However, we have decided to take several unusual steps to limit our exposure, including refraining from making our paper available to other researchers before formal publication; this is not in the best interests of the field, and it is not our usual practice, but we do not feel comfortable with the risk.

66. After spending this much time worrying about the DMCA, I have concluded I cannot afford to work in any area that exposes me to such risks. The costs are simply too high:

in our research on HDCP, I spent more time speaking with lawyers than I spent on the scientific research itself. And I cannot in good conscience advise students in my research group to work in areas that would expose them to unknown legal risks.

67. As a result of this experience with HDCP and the DMCA, I do not think I will ever conduct research involving copy protection again.

THE DMCA'S EFFECTS BEYOND COPY CONTROL

68. Unfortunately, because of the breadth of the DMCA, I am afraid that even more than research on specific copyright control technologies may be covered under the statute. Since any encryption scheme can be used as part of a system of access or copy controls, I am concerned that any cryptographic research that discovers flaws in encryption schemes could become potentially subject to the DMCA. Many encryption algorithms are designed for general-purpose use, and in many cases it can be difficult to predict in advance which applications a particular encryption algorithm may be used in today or at some point in the future.

69. If the DMCA had been in effect when we analyzed the flaws in Netscape's browser, we may not have been able to publish our results to the general public, which needs to understand the security of the software we use, or to scientific community without risking violating the DMCA. The exemption for reverse-engineering only applies for the purpose of enabling interoperability (i.e., for the purpose of getting the software to run on different platforms) and as I read the encryption exemption, it only seems to allow me to share research with the people with whom I am collaborating but apparently not to publish my results in a scientific journal.

70. The DMCA, had it been enacted earlier, might also have prevented our research group from ever discovering the flaws in GSM cellphones. Our research was enabled by the fact that a specific acquaintance with no formal training or credentials was willing to spend a few months reverse-engineering the GSM cryptographic algorithms for us. This allowed us to then analyze and find defects in these algorithms. Because there are serious reasons to doubt this collaborator would have been covered by the "encryption research" exemption, I am not sure that our acquaintance would have been willing to do the reverse-engineering work in today's world. We could not do the reverse-engineering ourselves (it was too time-consuming for an academic researcher), and our analysis project was impossible with access to the reverse-engineered information. The discovery of these flaws in GSM cellphones used by 50 million users worldwide educated the public, allowed industry to begin fixing the flaws, and has informed the way that next-generation cellular standards are designed, yet these flaws might still be unknown today if the DMCA had been passed a decade ago.

71. There are reasons to be concerned that the DMCA might reach farther still: Firewalls, for instance, effectively control access to a work protected by copyright, yet firewalls are a very important means of securing computer systems and an important object for scientific study. It would be difficult to over-emphasize the importance of being able to

circumvent these mechanisms in my research. (Firewalls are just one example, and in fact access controls pervade a large fraction of security systems.) If the DMCA were read broadly to prevent this type of circumvention, I would be concerned that I may have to abandon about half of the security research that I do.

I declare under penalty of perjury that the foregoing is true and correct and was executed at _______ on this the ____ day of _____, 2001.

David Wagner