Good morning. My name is Paul Hughes, and I am Public Policy Advisor at Adobe Systems Incorporated. On behalf of Adobe I would like express my appreciation for the opportunity to appear before you today at this important rulemaking hearing required by the Digital Millennium Copyright Act.

Before turning to certain specific issues raised by this rulemaking proceeding, I would like to talk about the critical importance of Section 1201 of the DMCA, and § 1201(a)(1)(A) specifically, to software companies like Adobe which confront a serous and pervasive piracy problem. The anti-circumvention rules enacted by the Congress in the DMCA are the results of a deliberate and considered response by the Congress to two facts: dissemination of works in digital form poses very real piracy threats to copyright holders; and the use of technological measures to thwart such piracy is needed to ensure the availability of legitimate copyrighted works.

Let me tell you a little about Adobe. Our history is an archetypal Silicon Valley entrepreneurial success story. Adobe's chairmen, John Warnock and Chuck Geschke, founded the company in 1982 with a modest business plan that envisioned employing 40 people working on a single software product. John and Chuck appear to have seriously underestimated their prospects, as Adobe PostScript and PageMaker went on to launch the desktop publishing revolution. Today, Adobe authors award-winning software for Web, print, and multimedia publishing. Its graphic design, imaging, dynamic media, and other software tools enable customers to create and deliver visually rich content across all media. Adobe is now the third largest personal computer software company in the United States, with annual revenues exceeding $1 billion. It is no exaggeration to say that Adobe would not exist in its current form were it not for the strong framework of intellectual property laws in the United States that has protected the creative work of all those who work at Adobe.

Markets for software markets are changing rapidly. With the establishment of the Internet as a major avenue for distributing software products, we see both a major business opportunity and a major potential threat. Software has the dubious distinction of being both the first copyrighted work distributed exclusively in digital form to which technological protection measures were applied, and also being the first type of copyrighted works to be exposed to massive digital piracy.

First, the opportunity. The Internet provides tremendous prospects for all types of products and services to be provided and distributed more quickly, more efficiently, and more cost-effectively worldwide. Forrester Research estimates that annual e-commerce sales just among businesses totaled $100 billion in 1999, and will reach $1.33 *trillion* worldwide by 2003.

Technology products, and software in particular, are leading the way in on-line distribution. IDC, one of the major research firms in the information-technology sector, predicts that the worldwide market for electronic commerce in software reached $3.5 billion in 1999and will grow to $32.9 billion by 2003, as more businesses and consumers become familiar with shopping on the Internet. According to some recent estimates, as much as 70 percent of software will be sold on-line by 2005.

Now, the threat. Unfortunately, like other criminals, Internet pirates are ingenious and adaptive, constantly finding new ways to adapt for illicit purposes the very technology that makes electronic commerce possible.

To give you a sobering example, if you do a search on the Internet today, you will find that over *2 million web pages* are offering linking to, or otherwise talking

about “warez,” which is the Internet code word for illegal copies of software. This rough indicator of the problem has increased substantially over the past three years, from 100,000 Web page hits two years ago, to 900,000 last year, and to over 2 million hits today. Virtually every software product now available on the market can be located on one of these sites, including all Adobe products.

To protect ourselves against pirates, the software industry has used a variety of technological protection measures. Often, these measures require a person loading a computer program on their system to enter a pass code or serial number as part of the installation process. If the wrong code is entered, the software cannot be installed or accessed. More recently, the industry has used a variety of encryption technologies. For example, to access certain anti-virus products purchased on line and downloaded, the recipient needs a decryption key, sent by separate –e-mail.

As the marketplace for computer programs has developed, it has also become the practice of most developers of business software products to license these works to their customers. This has proved to be the most efficient means of making these works available to both vendors and consumers. A business or other user will often receive a single copy of the work, and the license will authorize the use of that product by a specified number of persons. This practice, often referred to as “site licensing,” is now an industry standard. To ensure that only authorized persons use the software, loading the specific copy of the work in a computer often requires the application of a serial number, password or access code, to ensure that the person is legally entitled to access and use the software.

Hackers have adapted. Today hacker sites offer serial numbers, access codes and software program “patches” that bypass or circumvent encryption or other technical protections that the copyright owner may have applied. Using a popular

search engine, and searching on the key word “crackz”, we recently found over 1,000,000 web pages which make available such “patches”—many of which are specifically designed to defeat these technological protection measures.

To give another example, an enterprising hacker has written a small utility program, the “Adobe Serial Number Generator,” that does what its name suggests. It will generate usable—but illicit—pirate serial numbers that enable access to our products and updaters by those who have not licensed legitimate copies of our programs. The making, distribution, and use of this pirate serial number generator is analogous to the selling of burglar tools or unauthorized satellite TV descramblers. The latter two categories of devices are illegal under state and Federal laws, and Congress intended to do the same with copyright circumvention devices—make them illegal.

From our industry’s perspective, § 1201(a)(1)(A) is an indispensable legal tool needed to prevent piracy and the distribution of these illegal access codes and patches designed to defeat technological protection measures.

We believe that it is self evident that the Congress recognized the critical nature of this cause of action. That is why it is part of the law, and why this Administration pushed hard for the anti-circumvention provisions of the WIPO Copyright Treaties that the DMCA implements. The fact that Congress saw fit to establish this rulemaking cannot be treated as an opportunity to overrule the will of the Congress. The consequences for Adobe, and for the software industry as a whole, would be disastrous.

The vast majority of the comments submitted suggest just that the anti-circumvention cause of action a whole should be suspended. We strongly

disagree. In addition, such a course of action is not within the scope of this rulemaking. More about this in a moment.

A great many other submissions argue that non-infringing uses of works, such as those contemplated the fair use provisions of the Copyright Act, somehow trump the copyright holders right to license and enjoy their property interest. Again, that issue is not the subject of this rulemaking, but much has been made of the supposed danger, such as the development of pay-per-use business models, which may develop if this cause of action goes into effect.

This argument that possible non-infringing uses of works deserve a higher level of consideration than the copyright owners' interests has been the subject of much attention recently, including recent litigation. We believe these arguments to be ill founded.

For example, in the recent *UMG Recordings Inc. v. MP3.Com*, MP3.Com made this very argument. Judge Rakoff had no trouble disposing of the argument. He wrote:

> Finally, regarding defendant's purported reliance on other factors (analyzing the four fair-use factors set out in § 107), this essentially reduces the claim that My.MP3.com provides a useful service to consumers… Copyright, however, is not designed to afford consumers' protection, or convenience, but rather, to protect the copyright holders' property interests. Moreover, as a practical matter, plaintiffs have indicated no objection in principle to licensing their recordings to companies like MP3.com; they simply want to make sure they get the remuneration the law reserves for them as holders of copyrights in creative works. Stripped to its essence,

> defendant's "consumer protection" argument amounts to nothing more than a bald claim that defendant should be able to misappropriate plaintiff's property simply because there is a consumer demand for it. This hardly appeals to the conscience of equity.

As Judge Rakoff makes clear, the goal of the Copyright Act is—in part—to enable copyright owners to license their works for a fee. There is nothing wrong or inappropriate about this. The fact that access control technologies facilitate such forms of commercialization of works is not only consistent with the intent of the Copyright Act generally, but the specific intent of Congress in enacting § 1201(a)(1)(A).

Turning to specifics, the goals of this proceeding are clearly spelled out in the statute and the relevant legislative history. Those who assert that the effective date of the § 1201(a)(1)(A) prohibition should be further delayed shoulder an extraordinarily heavy burden of persuasion. They must demonstrate, through "highly specific, strong, and persuasive" evidence, a likelihood that, over the next three years, the net impact of outlawing theft of passwords, unauthorized decryption, or descrambling, and similar acts of circumvention, will be to harm substantially the ability to make licensed, permitted, or other non-infringing uses of specifically defined "classes" of copyrighted materials.

The arguments present in the submissions and the oral testimony make a number of arguments why the cause of action should not go into effect. We believe that each of these fails to make the case required by the law.

Many submissions argue that § 1201(a)(1)(A) should not come into effect on October 28, 2000 for any class of work. We believe that this would have the same

effect as overturning the law through a rulemaking. That is clearly wrong. Had Congress intended that as a possibility, it would not have enacted the cause of action at all. The statute, by speaking about specific classes of works, clearly directs the Librarian to examine, on a case by case basis, the balance of interests in each instance. The case must be persuasive and compelling, and addressed to specific classes of works, and not to broad types of works, such as, for example, software generally.

A number of the submissions are devoted to arguments specific to the software industry. These submissions argue that § 1201(a)(1)(A) would impeded reverse engineering of software. The interrelation between anti-circumvention rules and acts of reverse engineering (legitimate acts of studying and analyzing a computer program), were considered in detail by the Congress in the course of its deliberations on the Digital Millennium Copyright Act. Section 1201(f), was added by the Senate during its consideration of the Act. That section is a specific exception to § 1201(a)(1)(A), and, thus, reflects the deliberate judgment of the Congress in respect of exceptions it determined to be appropriate. The legislative history of the Senate bill, makes clear that the specific intent of the Senate in adding § 1201(f) was to "…ensure that the effect of current case law interpreting the Copyright Act is not changed by enactment of this legislation for certain acts of identification and analysis done in respect of computer programs."

Section 1201(f) is not the subject of this rulemaking. Whether changes to § 1201(f) are appropriate (and we do not think any are needed) is a mater for the Congress, and the Congress has not directed this rulemaking to consider that issue.

I would like to make one final point. The vast majority of the submissions argue that truly bad things will happen if technological measures can be used to control

access to software and other works. But these arguments fail to recognize the fact that the use of such measures is not a new development. As I mentioned already, software developers have long relied on technological protection measures. Password and serial code controls have been in use for over a decade. Encryption technologies have been used for more than five years. Over the years, companies have made many changes in how they use these technologies, in part as a response to consumers' needs, and in part to thwart pirates.

The submissions filed do not argue that the use of these technologies has inhibited the availability of works, or harmed the legitimate user. Why do they do not argue this? Because there is no evidence to bear out such a claim.

The gist of the arguments made is that creating a cause of action against hackers of these technologies would change everything. While the submissions raise a vast array of hypothetical possibilities, none present compelling evidence that the ongoing practices have created a problem.

There is substantial evidence, however, that hackers are developing a posting patches and other means aimed at defeating these technologies.
Section 1201(a)(1)(A) gives us powerful weapon to fight back. That is what the Congress intended.

Adobe and BSA respectfully submit that, based on the submissions and testimony to date, the record fails to demonstrate that any "particular class of works" is likely to be subject, over the next three years, to a substantial adverse impact.
Section 1201(a)(1)(A) should take effect on October 28, 2000, as intended by the Congress. Thank you.