R. Michael Tanner
Professor of Computer Science, School of Engineering
University of California, Santa Cruz

Testimony before Representatives of the United States Copyright Office
February 10, 1999
Los Angeles, CA

I am Michael Tanner, a member of the faculty in the Department of Computer Science in the School of Engineering at the University of California, Santa Cruz. My particular expertise is in theories of error-control coding for message preservation. The amazing success of digital coding in allowing flawless transmission and replication of digital materials has intensified examination of copyright protections I also recently completed a nine-year assignment as Executive Vice Chancellor, the chief academic officer of the Santa Cruz campus, where I was active in promoting the use of information technology in innovative teaching.

You have heard from other university witnesses that our ability to develop the potential of distance education requires expansion of copyright law's existing exemptions for education. I will pursue that theme further. I will also underline that information technology is rapidly evolving, inviting creative new educational uses and at the same time, opening up unprecedented ways of protecting copyright holders' legitimate interests.

Expanding possibilities

Today's teachers' ability to reach a diverse array of students has grown dramatically since their earliest forebears relied exclusively on the spoken word in face-to-face settings. Generations of technological advances, from the printing press through television and the video cassette recorder to the Internet, have made it possible to serve ever more students with increasingly rich, eclectic, and informative material. Yet, technology alone has not been enough. Educators have required special treatment to take full advantage of new capabilities.

As the Internet and Java applets open up new vistas for education, publishers and other content owners express fear that expanded exemptions for digital materials used in networked distance education will adversely affect the viability of their businesses. Two factors contribute to this view: (1) fear that digital content released in an educational setting will be widely redistributed by students, and (2) a perception in some quarters that educators want "something for nothing." We can meet the first of these concerns by responsible treatment of the copyrighted material we use in education, as I will discuss in a few moments. We may disagree about the scope of the second concern, but I suggest that educators' use of copyrighted material in education helps create and expand markets by increasing students' awareness and understanding of these works, whetting their intellectual appetites for the original work in its entirety. And we need to emphasize that

many of the works we seek to use in classroom and networked environments are copyrighted but are not commercial properties.

Faculty investment

My experience as both a member of the faculty and an administrator persuades me unequivocally that faculty will not participate in developing the potential of the Internet for teaching if they cannot easily adapt what they now do in the classroom to the new medium. Tremendous creative effort goes into developing digital enhancements for classroom and independent student learning. Faculty must invest countless hours to develop animations that make pedagogic points, integrate sounds and images in multimedia modules, and develop links to selected Internet resources. It is important to note that much of the content faculty develop in this way is original. But, inevitably and necessarily, it also includes and references work created by others, in a process of incremental creation of new knowledge.

Most of this work is in addition to "ordinary" teaching and research obligations. Within the physical classroom, the educational exemptions have allowed faculty to focus all of this effort on intellectual and pedagogical issues. If the networked environment requires complex, time-consuming, and uncertain negotiation for permissions, or if faculty feel constantly anxious about infringing copyright, they will turn their attention in safer directions. Innovation will be stifled.

The loss would be significant if today's efforts to extend the classroom across digital networks were abandoned. In some disciplines, interactive learning outside the classroom now often surpasses that occurring in class, while faculty collaborations on and between campuses enrich the environments for graduate student research and undergraduate learning. Such collaborations can link different sites on a single campus, within university systems like that of the University of California, and in unrelated institutions. They are built on timely exchanges of ideas and criticism, revision, and introduction of new materials. Their potential to incorporate entire new constituencies of off-campus students is just beginning to be realized.

I do not want to spend time in alarmist speculation, however. Rather, I would like to draw your attention to important areas where the interests of educators and content owners converge.

Controlled access

Faculty and institutions alike have strong interests in controlling who has access to classes. The more interactivity is built into an online resource, the more care we will take to protect the privacy of participants. In addition to privacy, we are also concerned about demands for interaction that could overwhelm the faculty's ability to respond. Equally important, our institutions must maintain the quality and integrity of course offerings. Institutions also want students to pay enrollment fees and meet admissions requirements.

For all of these reasons, the general public is not offered free access to physical classrooms, potentially diverting attention and draining resources. The general public will not be invited to freely sample our online classes either.

We can assure copyright owners that material made available through educational exemptions will be contained within a limited community. We will cooperate with and respect limitations on copying and distribution. However, if such cooperation is unreasonably burdensome or intrusive, faculty will frequently choose not to use the material in question. Already, anxiety is high in academia about the kinds of demands proprietors will make in exchange for allowing their copyrighted material to be transmitted to students over networks. Stories of exorbitant prices and intrusive technologies that track individual use of copyrighted works distract and alarm faculty whose primary interest is in sharing knowledge and understanding with their students .

How, then, will we use the capabilities of the Internet for distance education without abandoning the principles of Fair Use or allowing large amounts of copyrighted material to be illegally copied and redistributed? Evolving technologies will help.

Technology in flux

Although various techniques for preventing piracy of copyrighted digital works are in the market today, no one dominant method is in wide use. In many applications there are no standards yet, and standards would be premature. Research on security technologies is very active, well beyond what is in commercial use. Future choices may well be more acceptable to consumers, more effective, and more flexible. Further advances and their incorporation into manufacturers' standards will allay the fear that distorts today's debate over the limits of fair use and the validity of exemptions.

It is worth distinguishing between the two kinds of protection that must be in place to ensure that copyrighted material used under the educational exemptions does not go into general circulation. First, measures need to be in place that limit access, so that the transmitted material is available only to authorized users, such as students enrolled in a class. Second, it must be possible to prevent permanent storage and redistribution of the material. Various models of access control technology are already in the market, and others are under development. These include both hardware and software approaches and range from strong encryption to weak protections based on passwords and IP addresses.

It is proving more difficult to develop practical ways to control what users can do with material once they are granted access. It is commercially viable now to place material on a server and allow it to be viewed or operated without being downloaded. But images and sounds can be copied from an output device (a monitor or speaker), so this alone may not satisfy the owners of materials such as motion pictures, images, and music. Techniques of hardware and software are in development that will prevent copying or retransmission of specific data, but those that rely on intrusive monitoring of user behavior or are excessively complex and expensive will not gain broad acceptance.

For some purposes, a restriction to low-resolution output may provide sufficient protection. This enables users to view or hear a version of a file that does not contain all its data. Just as a photocopied book is less convenient and attractive than the printed original, low-resolution copies generally will not substitute for the original.

Universities will use security technologies that are easy to apply and are available at reasonable prices. We have relevant experience: universities have been licensing high-end software for campus use for years. Our vendors will attest that we have managed these applications from central servers with few copying abuses. The software piracy that does take place on college campuses is not related to institutionally licensed applications. Moreover, university researchers are at the forefront of the basic research that will produce new technologies, and our computing staff have long been innovators in prototyping applications. Indeed, some of the distance education classes for which we wish to transmit digital material are aimed at computer and information science students whose work will contribute to this development.

"Good enough"

Finally, there will always be tradeoffs between levels of protection and the value to be protected. No reasonably priced commercially available security measure will be immune from determined attack by experts. Consumer technologies must rely on the assumption that most users will not invest heavily in acquiring skills and special equipment to thwart security systems. It simply will not be worth it.

As suggested above, technologies exist--or can be developed--to provide substantial protection for copyrighted material to which they are applied. Universities will use them in distance education settings to protect the interests of copyright owners. The fact that they can be broken by determined assault does not mean they are ineffective. Determined assault can be deterred by criminal penalties. In the meanwhile, publishers' willingness to license digital materials to our libraries indicates that reasonable safeguards for digital materials can already be implemented in some circumstances.

In sum, then, development of the great opportunities the Internet offers for distance education requires that the exemptions currently offered for classroom teaching be extended to the networked environment. As technology develops to ensure that these exemptions will not be abused, educators and publishers need to work together to establish appropriate levels of security for various kinds of material. The educational exemptions have served publishers and educators well by carving out a special territory against the backdrop of owners' exclusive rights and fair use. These exemptions need to be extended to legitimate distance education in the networked environment.