House Committee on Science and Technology
The role of technology in reducing illegal filesharing: A university perspective
June 5, 2007

Dr. Adrian Sannier
University Technology Officer
Arizona State University

Thank you, Chairman Gordon, Ranking Member Hall, and other Members of the Committee for giving me an opportunity to describe for you Arizona State University's use of technology to reduce the incidence of copyright-infringing filesharing on its campus networks.

As one of the nation's largest universities, with over 65,000 students attending its 4 campuses in the metropolitan Phoenix area, ASU provides its students, faculty and staff with an extensive and evolving array of computing and communications services. These services have become a core enabler of the University's academic and research missions.

To govern the legitimate use of these services, ASU developed an Acceptable Use Policy for its computing and communication services that expressly forbids their use to transfer or exchange files when that transfer or exchange would infringe on copyright. Users of the University's computing and communication services must electronically agree to this policy as a condition of connection. The policy explicitly forbids the use of university communications or computing infrastructure for any unlawful communications, including "threats of violence, obscenity, child pornography, copyright infringement and harassing communications".

I am pleased to report that, despite some news reports to the contrary in the popular press, ASU has a relatively low rate of complaint about the illegitimate use of its network from copyright holders such as the RIAA. ASU's complaint rate, which is the number of individuals alleged to have distributed copyrighted content per thousand students, was only 0.52%, the lowest among the 25 institutions for which the RIAA released data this past Spring.

In a recent letter to University Presidents around the nation, the RIAA outlined a set of four best practices that they recommend universities employ to prevent or reduce student exposure to lawsuits and/or Digital Millennium Copyright Act notices. ASU was an early adopter of each of these best practices, and they are the cornerstones of ASU's successful containment efforts.

The first recommended practice is to educate students about the do's and don'ts of downloading and copying music and other copyrighted works. ASU incorporates these topics as part of our new student orientations, our residence hall orientations and our twice yearly information security week orientations.

The second recommended practice is to offer students a legitimate online service, one that provides an inexpensive alternative to illegal file-sharing. Beginning in July of 2005, ASU was an early adopter of one such service, a digital entertainment network designed specifically for college students known as Ruckus. ASU's subscription provides its students with downloadable access to 2.75 million songs, full-length feature films, short-form video, sports clips, and music videos, as well as access to a social network site focused on the network.

The third recommended practice is to take appropriate disciplinary action when students are found to be engaging in infringing conduct online. Under the terms of ASU's Acceptable Use Policy,

> *upon receiving notice of a violation, ASU may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings. A person accused of a violation is notified of the charge and has an opportunity to respond before ASU imposes a permanent sanction.*

In addition to sanctions available under applicable law and ASU and regents' policies, ASU may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, ASU-administered computing rooms, and other services or facilities.

The RIAA's final recommendation encourages universities to implement a network technical solution to restrict, filter, or curtail peer-to-peer file sharing. Any technical solution must balance the rights of copyright holders with the legitimate uses of the university's network and its users' expectations of privacy and academic freedom.

Beginning in December of 2000, ASU's first attempt at a solution was a network monitoring solution from Packeteer. ASU used the Packeteer product to monitor network data streams and use the protocol information contained in the streams to prioritize traffic. This allowed ASU the amount of university bandwidth devoted to peer-to-peer traffic to be strictly limited. Over a five year period, ASU invested more than $250,000 in the installation and maintenance of this solution, which was purchased and maintained solely for its role in protecting the interests of copyright holders. In 2006, as the legitimate traffic volumes continued to increase, requiring a concomitant increase in investment in Packeteer, ASU began to look for a different solution.

After evaluating several different products and approaches, we have finally settled on Audible Magic's CopySense Network Appliance. The CopySense product does not disable peer-to-peer networking services or restrict the bandwidth available to them. Instead, the CopySense Appliance treats copyrighted material as if it were a computer virus on a P2P network. It works by blocking the exchange of copyrighted content while allowing legitimate files to transfer unobstructed. While our technical team was skeptical of the approach at first, our initial tests convinced us that the CopySense approach would provide us with a viable solution.

We installed the CopySense in spring semester without fanfare. It was configured to reject any traffic identified as registered commercial music, likely commercial music, likely commercial film and TV, or likely commercial software. It began rejecting about 5% of the overall network bandwidth immediately, identifying that traffic as the exchange of copyrighted material. Despite the interruption in network transmission, there was no noticeable increase in calls to our helpdesk, and we received no complaints about network performance for legitimate purposes attributable to the CopySense product.

Overall I would classify our adoption of CopySense as one of the easiest technical adoptions we have undertaken and that it has thus far caused very little disruption in our community.

The list price for the CopySense product at ASU's scale is just over $200,000, but ASU expects its costs this year, as a Pioneer Reference Account, to be closer to 1/2 that price.

While we at ASU are pleased with our new technical solution, we remain concerned about the potential for an ongoing "arms races". Peer-to-peer services have evolved to defeat effective counter-measures before and it would be foolhardy to believe that no further evolution is possible. As long as this "arms race" continues, universities will continue to be called upon to spend scarce resources procuring and deploying the latest technical counter-measures and expending time and energy in the protection of copyright at the expense of the value-added application of emerging technologies to the core missions of the institution.

We therefore applaud the progress that Apple and others have made in developing new and more effective business models for the consumer friendly distribution of electronic content and look forward to the day that these improved services make copyright-infringing file exchange unattractive to all but the fringes of our community.

Thank you again for the opportunity to share Arizona State University's experience with you.