Statement of Vance Ikezoye
President and CEO, Audible Magic Corporation
Before the House Science and Technology Committee
June 5, 2007

Good afternoon, Chairman Gordon, Ranking Member Hall, and distinguished members of the Committee. My name is Vance Ikezoye and I am President and CEO of Audible Magic Corporation. Thank you for your invitation to appear today to discuss the important issue of using technology to reduce digital copyright violations on university and college campuses.

By way of background, I am a co-founder of Audible Magic. I have a Bachelor's degree in Engineering from the University of California, Berkeley and a MBA from the University of Pennsylvania, Wharton School. My work experience includes 13 years at Hewlett-Packard. Audible Magic was founded in 1999 and is based in Los Gatos, California. We provide technologies, services, and easy-to-use solutions to identify and manage electronic media, including preventing its piracy. Our customers include legitimate peer-to-peer networks such as iMesh and Kazaa, and video sharing and social community sites like MySpace and Microsoft Soapbox. Artists, publishers and content owners desiring to protect or manage their copyrighted music, video or software register in Audible Magic's continually updated database. The electronic fingerprint and ownership information database currently exceeds 5 million works and is one of the largest collections of its kind in the world. My testimony here today is intended to provide an overview of the technological aspects of this issue, not to advocate a specific public policy position.

Audible Magic has developed a technical solution called the CopySense Appliance. Our product provides universities the ability to automate the education process, enforce network-use policies related to copyright, while protecting students' privacy and academic access to technology.

Technology's Effectiveness on Campuses

We introduced this solution in late 2003 and to date have over 80 customers worldwide including about 70 university and college customers. Our university customers span all corners of the United States and range in size from as few as 150 students to large public universities. In addition, we hope to soon have one of the highest enrollment universities in the United States as a customer. Both private and public institutions use the CopySense Appliance as a solution to illegal peer-to-peer file sharing on campus. Our experience in over 70 universities and colleges has shown that use of technology such as CopySense has significantly reduced piracy on campuses. On one college campus, we saw within one month an 80% decrease in total network traffic, a 71% decrease in the number of users of peer-to-peer file sharing applications, and finally the peer-to-peer file sharing traffic dropped from 20 GB per day to effectively zero in less than one week.

The CopySense Appliance was designed to intelligently detect and manage copyrighted content transfers over networks by individuals using popular public file sharing applications like BitTorrent and Gnutella. Since 2003, we have continued to improve our product and have focused on developing features to support the needs of universities and other educational institutions. Our solution is a turnkey, hardware product that is easily installed on the network of a university and provides automated detection and enforcement of copyright policies that are defined by the university administration. I will talk later about the new features we have integrated which provide tools to support the education of students in this area of copyright.

Using our copyright identification technology, the system matches unknown files transferred over known public peer-to-peer file sharing applications to a database of copyrighted materials that have been registered by the copyright owners. Since we focus on known public peer-to-peer file sharing applications, private communications such as email pass by unaffected.

Our design philosophy is based upon the belief that peer-to-peer file sharing technology is not the problem. In fact, peer-to-peer technology is powerful and will be utilized increasingly in mainstream applications in the future. Peer-to-peer file sharing networks themselves are an efficient means to distribute legitimate materials such as Linux software or even promote local unsigned artists' music. However, it is the unauthorized transfers of copyrighted works, whose owners do not want their works copied that is the problem.

Our product allows the technology to work for everyone. The system can be used to allow content owners, such as a local garage band, to designate their content to be freely distributed, while a major label or movie studio could designate their content to be blocked from distribution. All other content passes through unimpeded without affecting the network's performance or reliability.

Our product ranges in price from $5,000, on a small network, to $100,000 for a large university network, depending on the network bandwidth managed. Our customers have found that we can provide a cost-effective solution that can save them significant costs of bandwidth while providing better service to their users. As an example, one of our customers is a small technical high school, which uses a DSL connection, like many people have in their homes, and it found our product to dramatically improve its users' satisfaction in a cost-effective manner.

New Tools to Support Education of Students

I would like to highlight for the Committee the new capabilities of the CopySense Appliance, introduced this year, which are specially designed to support universities in their mission to educate students. The CopySense system provides universities the ability to influence student behaviors through a graduated series of student communications and sanctions. The CopySense system can detect students' violations of the university's network policies and apply automated sanctions to the violators, which are defined by the university administration. The university can configure the product to detect specific behavioral violations, which can include using peer-to-peer applications to download copyrighted music or movies.

Upon detection of these violations, the system will communicate with the student by automatically redirecting the student's Internet browser to a website which the university maintains. This website can be used to educate the student on their violation and the reasons why their behavior was inappropriate – these pages could even be used to administer a web-based copyright lesson and test. Because the system triggers at the time of the violation, the system is able to leverage the ‘teachable moment’ by immediately providing feedback to the student.

The system possesses a configurable point system that provides an escalation in the notifications or sanctions. As an example, if a student was a serious repeat offender, the system could block the student’s web, email, or Internet access for preset periods of time.

The system could be configured to direct communications privately to the student violating the school policy. Any other information or reports could be restricted from access by others unless configured and specified by the University. In this way the system can comply with most universities’ privacy policies.

Concerns About Technical Effectiveness

Before I get into specific issues that are commonly brought up about network technologies, I would like to point out that no technology is or will ever be a 100% effective solution no matter what the context. But I will also propose that a solution does not have to be 100% to be effective and make a difference on campuses.

Our design principle is that the system should not be over-reaching. Adopting this design principle, by definition, says that our system will not be a 100% solution. As an example, we may not be able to identify or even detect 100% of the file sharing traffic on the network. In order to detect 100% of the traffic, our system would have to be installed on every segment and device on the network – and this could dramatically increase costs. However, as I suggest, if we focus on feedback in an effort to educate students, we might begin to achieve the end result of correcting improper behaviors.

A critical concern of any technology relates to privacy. We have designed the CopySense system so that it can be configured to restrict access to information in a manner consistent with a university's privacy policy. If so configured, the university could treat this system as a black box as they do their other network equipment. This black box operates automatically without access by unauthorized personnel. In this way, the system's educational features could be configured so that only the student is notified of detection of their inappropriate behavior.

The second aspect of the system design with respect to privacy is that the system matches only copyrighted items in a database that are transferred over known public file sharing networks. All other communications such as email and web traffic go by unimpeded and without inspection. Our product operates in a manner similar to anti-virus products or even spam filters. Only our registry contains fingerprints of copyright works rather than fingerprints of viruses or spam.

From one perspective, our product is much less invasive from a privacy point of view than spam-filtering technology. Our product only detects the transfer of copyrighted works over public file sharing networks. Remember that these networks connect millions of anonymous strangers who are revealing the contents of their computers' hard drives; it is a question if there is even an expectation of privacy under these circumstances. Contrast that with spam-filtering technologies, which scan and intercept private email communications between known individuals.

One issue we hear from larger universities is the concern that our technology cannot handle the high-bandwidth speeds that they have deployed on their campuses. First, from a network administrative point of view, our system is not an inline device. Inline devices are problematic since all the data traffic needs to go through them. If the device is not fast enough or even worse, fails, it can slow down or stop network traffic. As a device that is not inline, the CopySense appliance operates on the sidelines and performs its matching activity in parallel with the real time network traffic flow. The actual experience of our university customers has been that the CopySense appliance has no adverse impact on network performance.

Secondly, we often get questions about our effectiveness – how can we match and identify files quickly enough to stop the transmissions of offending files when the campus networks are so fast? We have designed a very sophisticated solution to this question. Let me briefly explain both the concern and how we handle it.

Files transferred over networks are broken up into discrete chunks referred to as packets. In order to make a match using our technology, a portion of the file will need to be reassembled and a number of packets collected and buffered. Our system in the course of its operation does this routinely. Once we collect and reassemble enough of the file, we can perform a match using our fingerprinting technology.

You might be thinking, "This must take a long time and so on high-speed networks the system won't ever match a file before the offending file transfer has already occurred". Our technical approach isolates this problem to only the first time we see the file being transferred.

The first time our product comes across a file we have never seen before, we must go through the process of collecting and analyzing the file using our fingerprinting technology. As one might guess, on high-speed networks it may happen too fast for our technology. However, after this initial experience with the file, we can associate the identity of the file with an identifier, which is like an ID number for files shared over these networks. This ID number can be read from the data transmission very quickly – in more than enough time to take action. We maintain a local list of these identifiers in every system installed. Thus in most cases, this list can be used to accurately match files transferred even over high-speed networks in plenty of time to react.

I also want to point out that our CopySense content identification solution has become the industry standard, not only in the university network community, but in other technology settings, including legal peer-to-peer systems and user-generated content websites like MySpace, GoFish, and others. One of the many reasons why our technology has been adopted is because it is highly accurate.

A general concern raised about any network traffic analysis is the issue of encrypted file sharing networks. Encryption is a technique that is commonly used in electronic communications to scramble what would otherwise be an open, readable message. Encryption is most commonly used in financial transactions over the Internet, such as a credit card transaction, in order to protect the privacy and security of these transactions.

Peer-to-peer file sharing applications have adopted encryption, however, not to protect the privacy of the users, but to inhibit network management of peer-to-peer traffic and to prevent detection of illegal transfers of copyrighted-content files. The reality is that encryption technology can prevent the detection of content transfers at the file level such as that performed by our product. There are popular file sharing applications that use various levels of encryption today. However, even peer-to-peer file sharing applications that encrypt data often have some unique characteristics that identify the transfers. Our product deals with this by providing the university the ability to detect and block the use of encrypted peer-to-peer file sharing applications. This in combination with the educational features of the system is intended to discourage use of encrypted file sharing applications and migrate users back to unencrypted file sharing applications.

The term "darknet" generally refers to file sharing application networks that limit themselves to a local area such as a floor within a dorm. These darknets provide students a mechanism for transferring copyrighted files without exposing their illegal conduct to the university network systems or to the "light" of the outside world. The strategy to address this usage is to understand that detecting and stopping all darknet traffic is not the primary goal. The goal is to change the students' behavior. Therefore even statistical detection, perhaps by periodically deploying systems around the campus network, like a radar speed detection trailer that is moved from neighborhood to neighborhood, can be an effective means to influence students' behavior.

Can technology solve the problem of piracy of copyrighted works in every instance? Can technology clear all university and college campuses of illegal peer-to-peer file sharing? Technology will never be the entire solution. Technology is just one of the essential tools to combat piracy on campuses, and as the title of this hearing indicates, technology CAN reduce the number of violations and play a major role in supporting universities' and colleges' efforts to address this most important issue.

Thank you for the opportunity to appear before you today and I will be happy to answer any questions you may have.

Biographical Information

Vance Ikezoye co-founded Audible Magic in 1999. He has over twenty years of experience in high technology sales, marketing, and technical support including thirteen years at Hewlett-Packard Company. At HP he was involved in both the computer systems and medical products businesses. After HP, Ikezoye joined Trade Reporting and Data Exchange Incorporated, a VC-funded information company startup, where he served for five years in the positions of Vice President of Sales, Marketing, International, and Business Development. During that time, he developed distribution channels in the U.S., Europe, South America, and Asia. Ikezoye holds a Bachelors degree in Engineering from U.C. Berkeley and an MBA from the University of Pennsylvania, Wharton School.