From:	[redacted]
To:	FN-OMB-IntellectualProperty
Cc:	[redacted]
Subject:	Audible Magic - Submission of comments on the Joint Strategic Plan, REF: Federal Register / Vol. 75, No. 35, page 8137
Date:	Tuesday, March 23, 2010 6:40:14 PM
Attachments:	OMB_IPEC_Response.pdf

To: Office of Management and Budget
Intellectual Property Enforcement Coordinator

From: Jim Schrempp
Audible Magic Corporation
985 University #35
Los Gatos, CA 95032

23 March 2010

RE: Comments Regarding the Joint Strategic Plan

In the Federal Register / Vol. 75, No. 35, page 8137, the OMB IPEC requested submissions from the public regarding the Joint Strategic Plan for the Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement.

Written comments from Audible Magic Corporation are attached to this email in PDF format.

If you have any difficulty reading the attached file, please contact me directly.

Please be so kind as to reply to this email indicating that you have received our submission.

Best Regards,
Jim Schrempp
VP Engineering
Audible Magic Corporation
408.399.6405 x212

Audible Magic Response to the

Office of Management and Budget, Intellectual Property Enforcement Coordinator

Request for comments and recommendations on the Joint Strategic Plan and the U.S. Government's intellectual property enforcement efforts

22 March 2010

Deliver via email to: IntellectualProperty@omb.eop.gov

Direct comments or questions to:

Audible Magic Corporation
985 University Avenue #35
Los Gatos, CA 95032

408.399.6405
info@audiblemagic.com

Table of Contents

1. Purpose of this document

In the Federal Register, Volume 75, Number 35, page 8137, the OMB office of the Intellectual Property Enforcement Coordinator ("IPEC") issued a request for written comments from the public on the formulation of the Joint Strategic Plan ("JSP") and on the U.S. Government's intellectual property enforcement efforts. This document is the submission from Audible Magic Corporation ("AM"). In this document we will offer our perspective on some elements of the IPEC request for comments.

2. About Audible Magic

Audible Magic Corporation provides information services for media with a focus on the identification of intellectual property in a digital form. AM has a number of products and services currently in production used by

- over 75 educational institutions to manage peer-to-peer traffic on their network, such as Arizona State University, University of Florida, University of Chicago;
- over 25 major Web 2.0 audio and video sharing sites to enable monetization and copyright compliance, such as MySpace, MTV Networks, Facebook;
- over 25 CD/DVD replication companies to quickly and accurately inspect newly submitted master disks for intellectual property issues;
- the entertainment industry trade associations for fast and accurate identification of content, such as the Recording Industry Association of America (RIAA), and the International Federation of the Phonographic Industry (IFPI).

Audible Magic is a leader in the market and as such has provided comments in a number of governmental and regulatory settings including: testifying before the Science and Technology Subcommittee of the U.S. Congress; submitting an amicus brief with the U.S. Supreme Court in the case of MGM v. Grokster; testifying at an U.S. Federal Trade Commission hearing; and participating in a variety of other public discussion panels.

Audible Magic holds 8 U.S. patents and 2 European patents. AM was founded in 1999 and is a U.S. Corporation.

Our company has in-depth expertise with certain aspects of intellectual property protection. Our comments come from this expertise. We are pleased to offer our perspective to the IPEC.

3. Part I of the IPEC request

Part I of the IPEC request asks for comments about the threat posed by violations of intellectual property rights. We have no comments to submit about this section at this time.

4. Part II of the IPEC request

Part II of the IPEC request outlined a number of objectives of the JSP. Our comments on these objectives are below. The relevant JSP objective is in red; our comments, in black.

- Identifying weaknesses, duplication of effort, waste, and other unjustified impediments to effective enforcement actions

  When an agency representative is presented with a suspicious set of CDs or DVDs it can be time consuming and may be impossible for agency representatives to determine if the disks contain infringing copies of musical performances owned by U.S. companies – with millions of owned musical performances it is impossible for any representative to be familiar with them all. In addition, two performances of a song may have different copyright ownership yet sound very similar to agency representatives.

  If agents were equipped with a tool to quickly and accurately identify disks containing the specific musical performances that are owned by U.S. companies, they could be more effective.

  Audible Magic sells a product called RepliCheck. RepliCheck is an easy to use software application that can quickly determine if a CD or DVD disk contains a copy of any performance registered with Audible Magic. All major U.S. music industry players register their performances with Audible Magic. To date over 7,000,000 performances have been registered; over 2,000 performances are added every day.

  RepliCheck can also be applied to quickly identify raw files found on the hard disks of laptops and computer servers. This can be useful to agents investigating computer systems they suspect may contain files that infringe on U.S. intellectual property rights.

  We suggest the U.S. Government equip agents with Audible Magic's RepliCheck software. This would reduce the time and manpower required to quickly and accurately identify U.S. intellectual property when they encounter it.

- Disrupting and eliminating infringement networks in the U.S and in other countries

P2P Networks Used for Infringement

Massively connected Peer to Peer ("P2P") networks are used world wide to distribute illegal copies of music, movies, software, and computer games. The U.S. music and movie industries have publicly claimed huge commercial losses due to these networks.

These P2P networks have legitimate use for the fast and far reaching distribution of public domain content.

Complete Elimination of P2P is Very Difficult

Once infringing activity has been detected, several actions are possible. One response is to attempt to disrupt the activity immediately, typically through the use of some network technique to break the link between two P2P clients. While this seems like a satisfactory solution, in fact it can lead to more infringement that is harder to detect. First, P2P technology has been designed to be resilient to just such a link failure and continues to infringe over other connections. Second, in response to the repeated use of this disruption, P2P software application developers changed the technical basis of their communication protocols to make it more difficult to disrupt.

Change P2P User Behavior Through Education

A focus on identifying infringing P2P users and changing their behavior through education can dramatically reduce infringement over P2P networks. In our experience the vast majority of P2P infringers will stop infringing if they receive communication that is directly tied to their infringing activity. While there will always be a small number of P2P users that remain hard core "pirates", our experience shows that infringing activity can be significantly reduced by focusing on the 95% of users who will respond correctly when they learn that what they are doing is illegal and engenders serious consequences.

Identify P2P Users That Infringe

Obviously, in order to educate and change their behavior, the infringing P2P users first have to be identified.

One way to do this is to join a P2P network as a peer, and then attempt to obtain infringing material from others. Once infringing material has been obtained, then the user can be identified and appropriate actions can be taken. There are two approaches to this work, "over-the-top" and "in-network".

Several organizations are doing over-the-top infiltration today. The nature of over-the-top infiltration requires these organizations to expose their own IP address to the P2P network. In response to this over-the-top infiltration, P2P networks have evolved

methods to detect and reject infiltrators. A common method is the automatic publication of lists of IP addresses that are believed to belong to the infiltrators. This requires the infiltration companies to obtain a huge number of IP addresses and routinely switch them. As a result over-the-top infiltration has become more difficult and costly to accomplish.

A better approach to infiltration is for the infiltration to be done in-network. An in-network solution is able to overcome the ability of P2P networks to detect the IP address of the infiltrator. In-network solutions also put the network operator in control of the situation. Rather than an over-the-top attack profile, an in-network solution is able to work in a collaborative way with the network operator.

An In-Network Solution to P2P Infringement

Audible Magic offers a service called the CopySense™ network appliance ("CSA") with Graduated Response that can play a key role in disrupting and eliminating infringement over P2P networks. The CSA is able to detect infringing P2P traffic as it transits the network.

While strongly respecting individual privacy, the CSA can identify just those P2P transfers that are infringing without any impact to legal content transfers. The CSA uses a standard network configuration that allows it to work in a manner that has absolutely no impact on the observed network. It is impossible for the CSA to introduce latency, jitter, packet loss, or become a network failure point.

The CSA can alert the network operator to infringing activity, and the network operator may begin a system of Graduated Response. It has been demonstrated on U.S. college and university campuses that when the CSA is deployed on their network, infringing activity drops dramatically.

Typically the first step in a Graduated Response to infringing activity is for the network operator to communicate to their end user in an appropriate educational fashion. After repeated infringements a network operator may choose to sanction the user in some way, such as limiting their bandwidth or the scope of their internet access or promoting a legitimate source of the works the user desires. Some university network operators have implemented a system of fines, where subsequent infringement events involve increasing fees. The point is that the CSA initiated Graduated Response process allows a network operator to implement a system of compliance that is best suited to their users, their customers, and their network.

Instant Messaging

Instant Messaging ("IM") is a way for two people to communicate in a private text based conversation. Current IM software also allows the participants to exchange digital files. These files could contain copyright protected material.

The use of IM has grown dramatically and infringement certainly occurs. However it is still focused on one-to-one or one-to-few communication. As such, the total amount of infringement over IM is small compared to the infringement of massively connected P2P networks with millions of users.

We believe many P2P users are also users of IM. As a Graduated Response system educates these P2P users to the consequences of infringing activity, the positive change in their behavior may also spill over to reduce infringement over IM.

Cyberlockers and Usenet

Cyberlockers began as a way of a user storing files on a remote system for later retrieval by the same user. Many cyberlockers now allow one user to upload a file and then provide a mechanism for other users to download this same file. It is possible for the file to contain copyright protected material. In fact, there are reports that some cyberlockers are being heavily used for distribution of infringing digital goods. Usenet can be considered a form of a cyberlocker.

Cyberlockers present a different target for interdiction than P2P networks. Cyberlockers have a centralized architecture to a large degree, while P2P networks are completely decentralized. Cyberlockers may replicate files or portions of files to provide redundancy and they may distribute some control functions, but they are fundamentally centralized. As such, cyberlockers incur significant centralized expense for systems and bandwidth. This expense must be borne by an organization. The most popular of these organizations are commercial entities charging users substantial monthly fees for access and bandwidth. Interdiction efforts can be aimed at these organizations.

From an infringement standpoint cyberlockers can be addressed in the same way the Web 2.0 industry was handled. Cyberlocker companies could use industry standard content identification technologies to scan their content repositories and restrict access to files with copyright protected so that only the original owner can subsequently download the file.

It should be pointed out that some cyberlockers provide client software which encrypts the files prior to uploading. In these cases the solution is similar to P2P clients – the software should have industry standard content identification embedded in it. Unrestricted downloading could only be allowed for files that have been tested and known to be free of infringing content.

Audible Magic offers a full set of robust, easy to implement identification services that could be used by cyberlockers to identify infringing activity.

Measurement of Efficacy

In a program like the JSP it is important to establish a measurement system to evaluate progress. The CSA can play a key role in this measurement system. CSA appliances can be deployed as passive monitors. They can be used to establish a base line of infringing behavior before different strategies are tried. Continuing reports from the CSAs can then objectively measure the effectiveness of the different interdiction strategies.

- Assisting other countries to more effectively enforce intellectual property rights

Graduated Response at Foreign Universities

As stated above, the CopySense network appliance is a powerful tool to identify infringing activity that takes place over a network. The service is not expensive, but cost is often a factor in deciding whether a network operator will deploy the solution. The U.S. government could provide incentives to other countries' educational institutions to encourage them to deploy the solution. Incentives could be as simple as paying for three years of the service. Other incentives could be used, such as providing U.S. educational opportunities to students from non-U.S. institutions that have deployed the CopySense solution. Other incentives could be proposed.

Physical Infringement

RepliCheck™ is an easy to use software application that can quickly determine if a CD or DVD contains a copy of any intellectual property registered with Audible Magic. All major U.S. music industry players register their performances with Audible Magic. To date over 7,000,000 performances have been registered; over 2,000 performances are added to the registry every day.

We suggest that the U.S. Government equip other countries' investigators and agents with Audible Magic's RepliCheck software pre-installed on laptop computers. This would increase other countries' capacity to quickly and accurately identify U.S. intellectual property when they encounter it.

5. Part II - Supplemental Comment Topics of the IPEC request

Part II of the IPEC request presented several Supplemental Topics that we will comment upon. The relevant Supplemental Topic is in red, our comments in black.

4. Provide examples of existing successful agreements, in the U.S. or abroad, that have had a significant impact on intellectual property enforcement, including voluntary agreements among stakeholders or agreements between stakeholders and the relevant

government.

Peer-to-Peer Software

In 2004 iMesh, a company that provides popular Peer to Peer software, agreed to cooperate with U.S. music industry copyright holders to prevent iMesh customers from using the software to infringe on U.S. music copyrights. iMesh included the Audible Magic media identification service in their client software. Each time an iMesh user downloads a file from a Peer to Peer network, the iMesh software uses the Audible Magic service to determine if the music industry has registered the audio performance with Audible Magic. If the performance has been registered, then iMesh directs their user to a source for legal download.

This unique cooperation between the stakeholders has allowed the iMesh corporation to flourish while providing strong protection of U.S. music industry intellectual property.

Web 2.0 Economy

In late 2007 several of the world's leading internet businesses (MySpace, Crackle, Microsoft, DailyMotion) and media companies (CBS, Fox, Disney, Sony, NBC, Viacom) announced support for a set of principles that allowed the growth of the Web 2.0 user-generated content ("UGC") industry while respecting intellectual property rights of the media companies. This landmark collaborative effort spelled out common objectives and specific steps the Web 2.0 sites could undertake to avoid infringing activity. The principles are available at http://www.ugcprinciples.com.

This mutual understanding of rights and responsibilities of both Web 2.0 sites and media companies reduced the enmity between these organizations and has led to new models of monetization and commerce.

Today major Web 2.0 sites, such as MySpace, Facebook, Crackle, DailyMotion, and others, use Audible Magic identification services to implement the UGC principles and enable commerce.

5. Suggest methods for strengthening information sharing between stakeholders and U.S. Government agencies to improve intellectual property rights enforcement efforts, including methods the U.S. Government can use to obtain more accurate information concerning the identities, corporate structures and locations of those suspected of intellectual property infringement.

Many infringing P2P transfers happen between computers in the U.S. and computers abroad. While the above mentioned CopySense network appliance is typically used by a network operator to open a dialog with their own users, strategically placed CSAs could be used to identify key P2P nodes in other countries. A CSA placed at the connection point between any U.S. network and the Internet at large (a so called

"peering point") can be configured to report on those computers in other countries that are involved in infringing activity. U.S. agencies could use this data to work with other countries to disrupt the world wide digital infringement network.

7. Describe existing technology that could or should be used by the U.S. Government or a particular agency or department to more easily identify infringing goods or other products.

Physical Goods – CDs and DVDs

When an agency representative is presented with a suspicious set of CDs or DVDs it can be impossible for agency representatives to know if the disks contain infringing copies of musical performances owned by U.S. companies – with millions of owned musical performances there are simply too many for any representative to be aware of. In addition, two performances of a song may have different copyright ownership yet sound very similar to an agency representative.

If agents were equipped with a tool to quickly and accurately identify disks containing the specific musical performances that are owned by U.S. companies, they could more easily and quickly identify infringing goods.

Disk replication companies face a similar challenge. When a customer presents a master disk for duplication, the replication company must exercise due diligence to ascertain that the customer has the correct license to allow replication. Audible Magic sells a product called RepliCheck. Since 2001, RepliCheck™ has provided a unique and effective solution.

RepliCheck is an easy to use software application that can quickly determine if a disk contains a copy of any performance registered with Audible Magic. All major U.S. music industry players register their performances with Audible Magic. To date over 7,000,000 performances have been registered; over 2,000 performances are added every day.

RepliCheck makes the identification using a patented technology (U.S. Patent #5,918,223) that works where so called "hash codes", "TOC" and other approaches do not. The world wide music industry uses RepliCheck in its own investigations.

RepliCheck could be a tool used by customs officials at all ports of entry. Customs agents could use RepliCheck to quickly inspect suspect shipments of CDs and DVDs into the U.S.

RepliCheck is the accepted industry standard for checking disks for infringing material. Audible Magic would enjoy the opportunity to provide the IPEC and other agencies with more detailed information about the software.

Application to Computer Files

RepliCheck can also be applied to quickly scan files found on the hard disks of laptops and computer servers. This can be useful to agents investigating computer systems they suspect may contain files that infringe on U.S. intellectual property rights.

Seeking Infringers

We imagine that government agencies may at times crawl (search) web sites or P2P networks in search of infringing activity. In these cases an agency will need to identify whether the media they discover is in fact infringing. Performing this test manually can be time consuming, difficult to do, and may be inaccurate. As mentioned above, the number of U.S. works that might be infringed is very large and media that sounds the same to an agent may have different copyright owners.

There are commercial organizations that crawl the web seeking infringers on behalf of copyright owners. Audible Magic provides identification services to these companies to make their work more accurate and productive. U.S. Government agencies involved in this kind of activity could also use identification services from Audible Magic to decrease manpower costs and improve effectiveness.

8. Suggest approaches for increasing standardization among authentication tools and technologies applied by rights holders to products to enable identification of these goods as genuine through a physical examination of the goods or product.

Many companies have a need for quickly determining the identification and copyright ownership of digital works. Audible Magic identification services provide a standardized method for determining ownership of musical and video works. Copyright owners register their works with Audible Magic. Entities that need to determine ownership use our services to do that. This market based approach to the problem has enabled organizations to quickly and efficiently obtain ownership information.

The U.S. Government could make use of this registry and associated services whenever needed.

11. Suggest methods to improve the adequacy, effectiveness and/or coordination of U.S. Government personnel stationed in other countries who are charged with enforcement of intellectual property…

Agencies investigating illegal CD and DVD replication in other countries could be equipped with RepliCheck on their laptops so that they can quickly demonstrate that suspect disks they discover do in fact contain the intellectual property of U.S. companies.

In addition, governmental agencies in other countries may be more cooperative with U.S. Government personnel if the U.S. personnel are using tools and procedures that also detect infringements of these other country's intellectual property. The Audible Magic musical intellectual property registry currently contains a significant number of performances that are owned by non-U.S. companies. By using RepliCheck to examine suspect disks U.S. personnel may provide agents of other governments with the motivation they need to pursue local action against infringers.

14. Suggest specific methods to limit or prevent use of the internet to sell and/or otherwise distribute or disseminate infringing products (physical goods or digital content).

P2P Networks Used for Infringement

P2P networks are used world wide to distribute illegal copies of music, movies, software, and computer games. The U.S. music and movie industries have publicly claimed huge commercial losses due to these networks.

These P2P networks have legitimate use for the fast and far reaching distribution of public domain content.

In our experience the vast majority of P2P infringers will stop infringing if they receive communication that is directly tied to their infringing activity. While there will always be a small number of P2P users who remain hard core "pirates", we believe that the amount of infringing activity can be significantly reduced by focusing on the 95% of users who will respond correctly when they learn that what they are doing is illegal and engenders serious consequences.

Audible Magic Solution

Audible Magic offers a service called the CopySense™ network appliance ("CSA") to network operators to solve this problem. The CSA is able to detect P2P traffic as it happens over the network. While respecting individual privacy, the CSA can identify just those P2P transfers that are infringing.

When infringing behavior is detected, the CSA alerts the network operator and the network operator begins a system of Graduated Response. Typically the first step is for the network operator to communicate to their end user in an appropriate fashion. This automated communication can reach the end user at a time when they are receptive to the message; the so called "teachable moment." If infringing activity continues then a network operator may choose to sanction the user in some way, such as limiting their bandwidth or the scope of their internet access.

It has been demonstrated on U.S. college and university campuses that when the CSA with Graduated Response is deployed on their network, infringing activity drops dramatically.

U.S. Government Networks

U.S. Government networks and those of affiliated agencies can also be the source of infringement. There have been widely reported cases of government documents that were inadvertently exfiltrated via P2P software running on government computers.

These reports lead us to believe that P2P software may be in use by government employees and contractors. It is possible for this use to be infringing. We suggest that a reasonable standard of diligence for network security would require the control of infringing P2P activity.

The U.S. Government could require that data networks used by its employees and contractors use CopySense network appliances to identify infringing P2P users. Agencies can then take appropriate action. This deployment can have a side benefit of reducing the inadvertent exfiltration of government data via P2P networks.

16. Discuss the effectiveness of recent efforts by educational institutions to reduce or eliminate illegal downloading over their networks. Submissions should include recent specific examples.

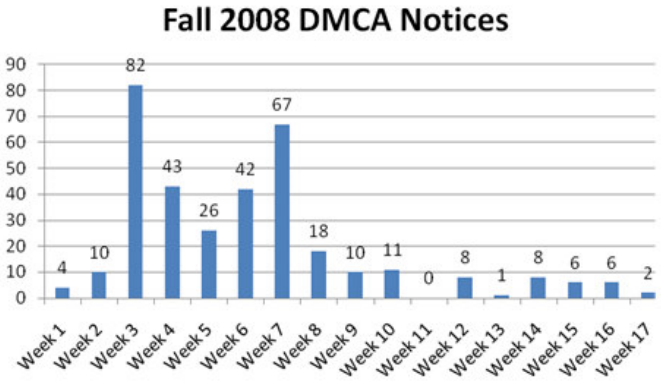
Schools and universities are common sources for obtaining infringing digital goods over P2P networks. Over 75 U.S. institutions have implemented the CopySense network appliance with Graduated Response as part of their digital citizenship curriculum to successfully curb illegal downloading over their networks. The CSA is able to find illegal downloading activity and automatically alert both the student and campus administration.

Campus administration then uses an integrated approach to turn an illegal download into a teachable moment. Typically the student is automatically directed on-line and in real-time to a short educational program on digital copyright and asked to stop their illegal activity. If the illegal downloading continues, the campus administration again informs the student and may take more significant steps to limit the student's bandwidth or scope of internet access. If the illegal downloading continues, the student may be referred into the campus judicial process. Some university network operators have implemented a system of fines, where subsequent infringement events involve increasing fees.

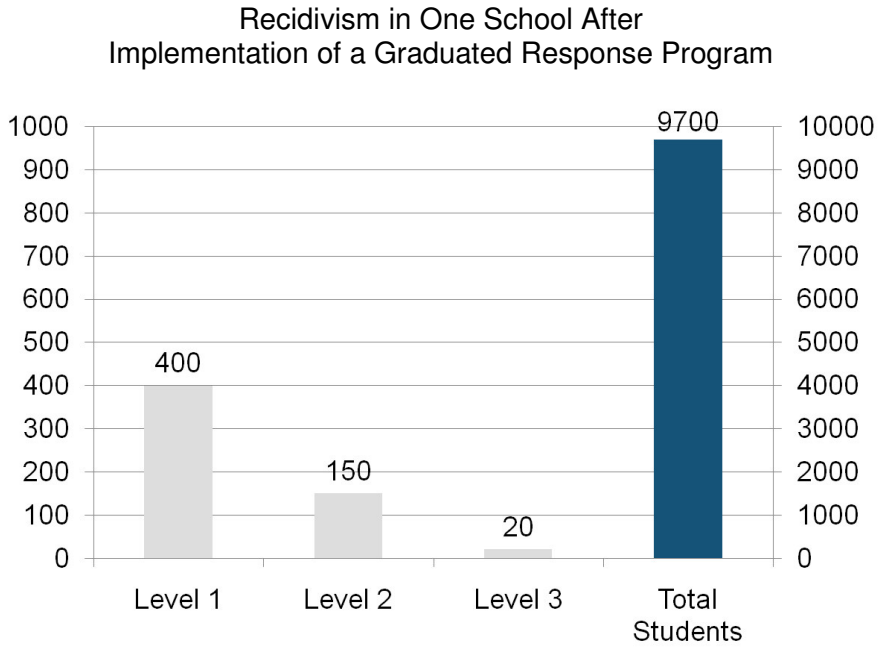
Additionally, most universities require the infringing user to signal their acceptance of the campus policy. They also provide an administrative contact to use if the user feels there was a mistake and would like to ask for a review of the infringement detection.

All this communication to the student and the structuring of the Graduated Response process is completely under the control of the university.

In one U.S. university, the number of DMCA takedown notices dropped 82% after the introduction of a graduated response educational system.



A system of Graduated Response provides a programmatic method of applying proportionate action for more serious abusers rather than treating all users the same. Most universities in the U.S. use one or more levels of infraction, with increasingly severe sanctions at each level. Some universities may restrict the users' internet access at some point. Other universities will quarantine the user and direct their traffic through a more constricted network. Other universities may fine the user nominal amounts. The use of a Graduated Response system in U.S. universities demonstrates its effectiveness in not only reducing total infringing activity but in reducing recidivism. The results from one school are shown below:



The experience of educational institutions using the CSA Graduated Response is exceptionally good. Campuses report that students who reach the first level of Graduated Response comply quickly and stop their illegal downloading over the campus network. For those students who do continue to the second step in the Graduated Response system, the vast majority stop their illegal downloading. Only a small percentage of students need to be informed a third time.

Audible Magic has a long history of successes with the CSA and would enjoy the opportunity to provide the IPEC and other agencies with more detailed information about the service and specific success stories within the U.S. educational community.

19. Suggest specific strategies to significantly reduce the demand for infringing goods or products both in the U.S. and in other countries.

Audible Magic's experience with universities has demonstrated that a focus on education and communication with customers is an effective mechanism to reduce the level of infringing behavior by users.

Education is most effective when it occurs in a timely fashion – i.e. communication occurs as close as possible in time to the infraction. Educators call this the 'teachable moment'. This communication can be accomplished using detection technology installed on the local network with automated communications to the user, all done without human intervention. We believe direct, timely communication to the user is the most effective way to reduce infringing behavior by the population at large.

Audible Magic's solution can integrate with a network operator's user authentication systems to implement this communication process. By providing alerts when infringing activity is detected, AM's solution provides the network operator with unlimited flexibility in how they communicate to their users.

Another component to reducing the demand for infringing goods is to provide users easy access to legitimate content; this is an important policy consideration. Every user that tries to download infringing media from a P2P file sharing network is a potential customer.

We believe there are many ways to meet the needs of consumers in a manner that will dissuade them from infringement. Other countries have been openly discussing a business model that bundles a range of media services into the consumer's monthly ISP billing. Recent press reports have speculated that the Isle of Man, and Virgin Media in the U.K. are both exploring this. In such a business model Audible Magic technology can be used in several roles. It can be used to identify works that are transferred over the network for subsequent back-office royalty splits. If the business model requires users to opt-in, then Graduated Response can be used to encourage infringers to sign-up for the media services.

20. Provide specific suggestions on the need for public education and awareness programs for consumers, including a description of how these programs should be designed…

As discussed above, we believe that communication to the public should be as close in time as possible to their infringing activity and be specific; these elements create a "teachable moment."

To take advantage of this teachable moment, an automated system built around the CopySense network appliance can construct the most appropriate message, personalized to the user. The communication can include specifics about when the infringement occurred and what was infringed; this demonstrates to the user that the message is not spurious. The communication can clearly state that the user's activity was infringing and state that the user should stop. Most users will. The communication should contain URL links that direct the user to easy to understand explanations of copyright laws and the user's personal responsibility.

Since infringing users are of all ages, the URL links should include a range of age appropriate information. From trendy, teen focused comic-like information panels to more serious education aimed at an adult population. The communication should include information on both copyright laws, user obligations, and the theory of fair use.

We believe a group of educators could be commissioned by IPEC to create this comprehensive copyright educational web site.

Of course, some users will continue their infringing activity. For those few users substantially more aggressive messaging can be taken.

6. Further information

For additional information on Audible Magic Corporation, the points of view expressed in this paper, the CopySense network appliance, RepliCheck, or other market ready solutions, please contact:

Jay Friedman
Vice President, Marketing
Audible Magic Corporation
985 University #35
Los Gatos, CA 95032

408.399.6405
E-mail: j_friedman@audiblemagic.com

