

# **Audible Magic**

Response to the RFI

From the  
Joint Committee of the Higher Education and  
Entertainment Communities Technology Task Force

*Technologies for Addressing Issues  
Associated with Unauthorized File Sharing  
on the University and College Campus*

## I. Introduction

Audible Magic has engaged in on-going research and development of content recognition technologies since 1994. In 1999, Audible Magic was granted its first U.S. patent (#5,918,223) for content-based analysis, storage, retrieval and segmentation of audio information. This patent led to successful development and delivery of multiple content recognition products utilizing audio & video fingerprinting techniques. With now 4 issued patents and 16 other patents pending, the company has significant advantages over its competition. Over time Audible Magic has also accumulated an authoritative audio and video fingerprint registry that is now one of the largest of its kind in the world.

Audible Magic is the leading provider of content identification services, with over 100 customers, processing millions of identifications per day in applications which track, protect and monetize copyrighted media titles around the world.

Audio and video fingerprinting has proven to be an exceedingly efficient and robust approach to identify multiple forms of media content, including video files. Most recently, Internet video-sharing sites have deployed Audible Magic's service as a means of managing copyright compliance

Audible Magic's future roadmap includes new patents and new developments in both audio and video fingerprinting technologies. Audible Magic is confident our own patented technologies and products delivery experience will continue to represent matchless industry leadership in all forms of content recognition.

## II. RFI Questions

### 1. *Features of the Technology*

Audible Magic's CopySense™ Appliance balances an institution's need to allow unfettered network access for legitimate research and education while at the same time effectively manage their network use policies against copyright infringement using file sharing technologies. Behaviors are the problem when it comes to infringing activities, not the technology; therefore the CopySense Appliance is designed to leverage technology to enable institutions to take advantage of "teachable moments." The flexibility of Audible Magic's technology enables a university to match the technology to their own unique set of network use policies and disciplinary actions.

The main features of the Copy Sense Appliance is to identify transfers of copyrighted content, which then enable opportunities for learning, educating students and other users on appropriate network use policies.

Of the six tool classes (audit, bandwidth shaping, data/file sharing blocking, matching/screening/filtering, user management & communication, and network performance), Audible Magic's CopySense Appliance integrates the data/file sharing blocking, matching/screening/filtering, and user management & communication into a single device. The appliance detects peer-to-peer file sharing traffic and then matches traffic using fingerprint technology against a database of fingerprints of copyrighted content. Based upon highly configurable options to structure actions to a specific institution's unique needs; the appliance may block streams; timeout internet activities; redirect users giving them warnings, quizzes, etc.; or just log when copyrighted material is transferred.

## 1.1 Network Architecture

The CopySense Appliance will connect within most network architectures. It is connected to an institutions network tap device at two points in a network: the Monitor Point and the Control Point. The Monitor Point is a place on your network that carries the network traffic you want to monitor. The **Control Point** is a place on your network that can be used to control the appliance via a web browser. If you ask the appliance to block certain kinds of traffic, then the Control Point is also used to issue blocking packets onto the LAN.

Below are three typical diagrams how the CopySense Appliance integrates with small, medium and large networks.

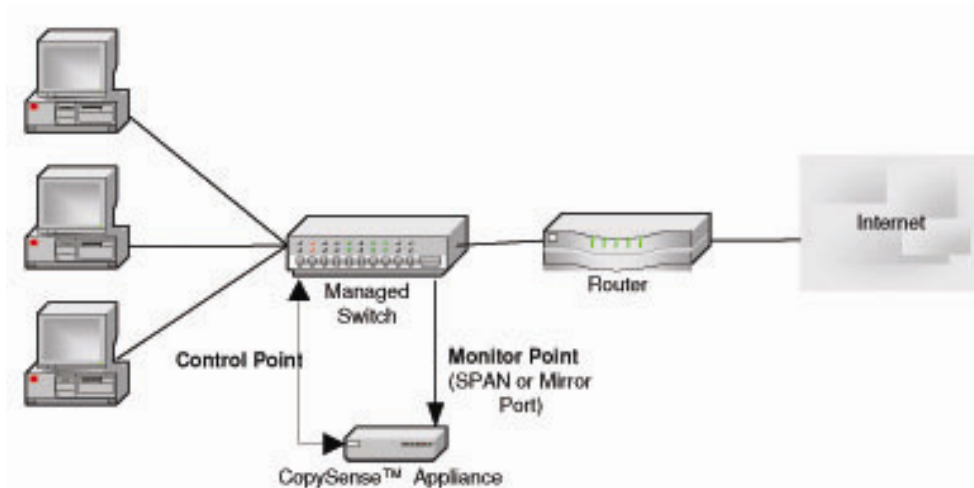


Figure 1: Medium network with a Managed Switch

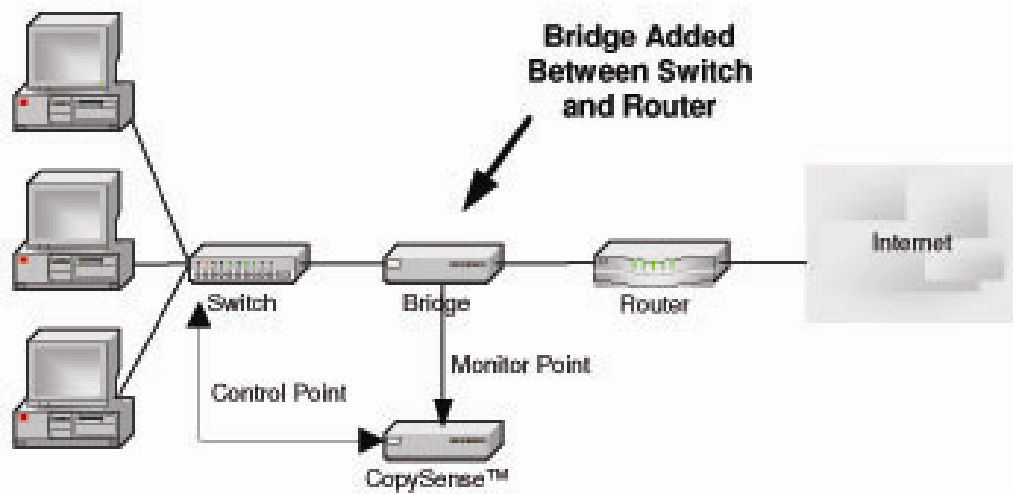


Figure 2: Small network with a bridge added

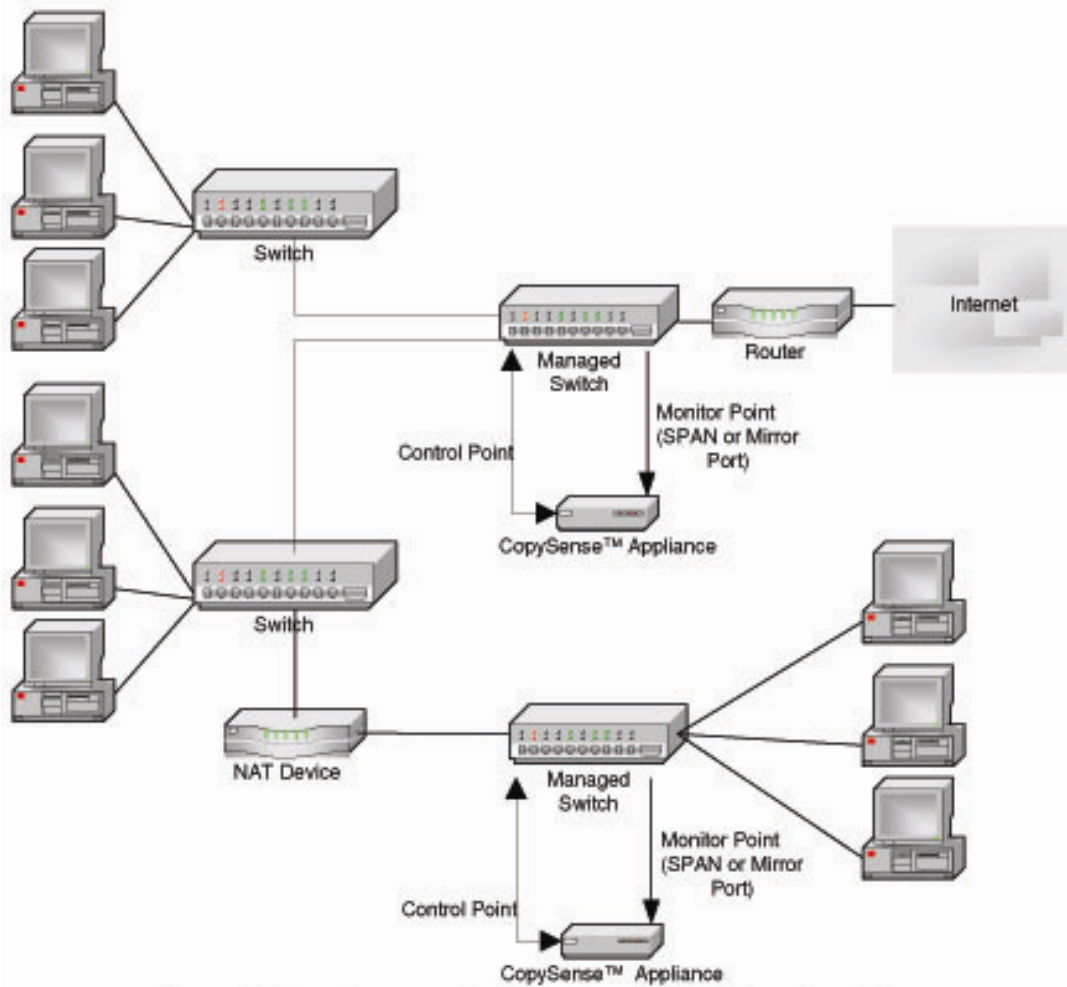


Figure 3: Complex network with a second CopySense® appliance

One advantage of the CopySense network appliance over other solutions is that Audible Magic's patented technology (*US Patent #6,044,402*) passively monitors your network. This means the appliance does not interfere with your network in any way. You could cut the cables to the appliance and it will have no effect on your network. It is **not** an "inline" device; it is a "pass-by" device. The appliance does **not** introduce any new failure points into your network. It does **not** slow down your network or introduce any latency.

The CopySense Appliance supports asymmetric networks, where network communication may be dynamically assigned different paths. Multiple appliances may be required along with our multi-module option that enables inter-device communication, thereby keeping each appliance current with the activities of all other appliance in the network.

## 1.2 Scalability

The CopySense Appliance may be configured to scale up to meet most institutions network capacity. For the largest implementations, the CopySense Appliance is offered with a load balancing solutions that can handle 10GB and larger networks. The multi-module option enables inter-device communication so that each CopySense Appliance is kept current with information about content it has identified by all other CopySense Appliances on the network.

## 1.3 Protocol Identification

The CSA uses various methods to accurately identify and monitor peer-to-peer communication, which is responsible for the vast majority of file sharing of copyrighted content (some consider >90% of illegal file sharing.). Actual detection methods are proprietary and further information on actual detection methods may be requested directly from Audible Magic.

## 1.4 Granularity of Protocols

Over 150 peer-to-peer applications and protocols, such as BitTorrent, LimeWire, Kazaa, Ares, eDonkey and many, many others are detected by the CopySense Appliance. Detection of new protocols and adjustments needed due to changes in each protocol is provided via daily updates. Detection can independently detect information during control sequencing, searching, uploading, and/or downloading/uploading of content, which can be independently set. As certain protocols are more aggressive than others, the appliance offers options to configurations based upon those applications which are more or less aggressive. Further information on actual applications and protocols detected may be requested directly from Audible Magic.

## **1.5 Product Configuration and Installation**

The CopySense Appliance requires less than 30 minutes to fully set-up, install, and configure. It requires virtually no downtime of an institutions network to install. The device is fully self-contained and other than connecting to the monitor and control points of a network tap device, such as a router or bridge, no disruption of an institutions network is necessary.

Only secured, authenticated browser access is allowed to the CopySense Appliance. No application or other components are installed on any other device, including individual PCs.

Except if a hardware failure occurs, no local maintenance is required. Daily updates are automatic. More significant software upgrades may require additional support.

## **1.6 Content Identification of Copyrighted Works**

The CopySense Appliance has several configurable methods for detecting copyrighted works. For most institutions, the appliance uses a proprietary fingerprint technology. The technology uses a fingerprint of a file being transferred, and then matches that fingerprint against a database of copyrighted works. Other configurable methods of detection include using control information (such as which P2P application or protocol is being used) and Bayesian filtering using associated meta data.

The appliance operates on most compressed audio formats (including recordings at various bit rates) and a wide range of video formats. The device communicates with Audible Magic's central registry/authority of commercially copyrighted content of Music, Film, and TV of registered fingerprints.

The device collects information regarding bandwidth (total and peer-to-peer), reporting of IP addresses transferring copyrighted information, as well as file name and other meta data reflecting actual copyrighted content detected.

Please contact Audible Magic if more specific information on the technology is desired.

## **1.7 Examination of Network Packets or File Content**

The CopySense Appliance technology fingerprints a file and matches that fingerprint against a fingerprint of copyrighted works. This technique is very similar to virus and SPAM filters many organizations require to be installed on their own networks. The appliance also optionally filters based upon control and associated meta data.

When infringing traffic of copyrighted content, information that is captured and reported includes: data/time of infringing traffic transfer, IP address where the infringement was identified, P2P protocol used, associated meta data, identification of the copyrighted work and file size.

## **1.8 Distribution Systems**

There are over 150 file sharing protocols and applications detected by the CopySense Appliance. The list below includes some of those detected – check with Audible Magic for an up-to-date, exhaustive list:

LimeWire/Gnutella  
uTorrent/BitTorrent  
Azureus/BitTorrent  
BitTorrent/BitTorrent  
BitComet/BitTorrent  
eMule/eDonkey  
Ares/Ares  
BearShare/Gnutella  
Shareaza/Multiple  
BitLord/BitTorrent  
KaZaa/FastTrack  
BitTornado/BitTorrent  
Frostwire/Gnutella

The CopySense Appliance detects peer-to-peer file sharing protocols. FTP, IRC, and other technologies may be added in the future. Check with Audible Magic for the latest technologies employed.

## **1.9 Resilience of the Technology to Countermeasures**

(Note that due to the sensitive nature of how the technology is designed which could be used to circumvent the appliance, limited information is shared in this section. Please contact Audible Magic if more detailed information is desired.)

Similar to virus and spam detection technology, every CopySense Appliance has access to the daily updates of copyrighted content and updates to new identification and detection methodologies. Audible Magic's engineering and support team continuously provide these new releases.

- (1) The CopySense Appliance is resilient to audio and video compression and some approaches to encryption.
- (2) The CopySense Appliance is able to detect copyrighted material in many use cases where user's efforts are made to thwart detection via tunneling, proxies, and fragmented packets.
- (3) The method of installation, authentication and that the CopySense Appliance is a passive listening device; therefore the appliance is resistant to outside attacks.

In Audible Magic's experience, the most effective use of the CopySense Appliance is for detection and education, leveraging the teachable moment. Although blocking may be employed, the opportunity to teach and educate may be lost.

## 1.10 Testing and Installed Base

Since 2002, the CopySense Appliance has been installed in real world environments at over 70 different institutions that includes small networks to very large networks at universities with enrollments of over 60,000 students.

Many different use cases are currently deployed by various institutions, such as:

- a. Graduated Response using a 3-strikes approach. This includes various approaches such as warning notices, implementation of quizzes, timeouts on Internet activity and others.
- b. Logging activity only when detection of copyrighted works are being shared
- c. Disruption of P2P traffic when copyrighted works are identified
- d. Disruption of all P2P traffic

In Audible Magic's experience, the most effective use of the CopySense Appliance is using the Graduated Response System with a 3-strikes approach, which leverages the teachable moment. Although blocking or disruption may be employed, the opportunity to teach and educate regarding the illegal activity of sharing copyrighted works.

All software releases are fully tested and run through Audible Magic's QA process to ensure the highest quality levels.

## 1.11 Competitive Approaches

Key benefits of the CopySense Appliance over other detection technologies include:

- a. Simple, Unique, Integrated Device – A single appliance includes all required components for most networks. Only large and/or highly complex networks may require multiple appliances to be installed.

- b. No additional points of failure are added to the network and the appliance is not susceptible to outside attacks – The CopySense Appliance is a passive monitor and is not an inline device.
- c. No additional network latency or jitter is introduced into a network – The CopySense Appliance is a passive monitor and is not an inline device.
- d. Largest Registry of Copyrighted Content – The CopySense Appliance has access to Audible Magic’s registry of over 7M unique fingerprints of copyrighted works.
- e. Allows unfettered access for legitimate Peer-to-Peer use – Using Audible Magic’s fingerprint technology combined with the registry database operates at a level of zero false positives.

### **1.12 Third-party Components**

Other than access to a networks tap device (router, switch, etc.), no third party products are required to use the CopySense Appliance.

### **1.13 Comparison with Hypothetical Scenario**

The CopySense Appliance handles and exceeds all capabilities of the hypothetical scenario. The capabilities integrated as part of the standard CopySense Appliance include:

1. Allow all legitimate traffic to flow through the network unimpeded
2. Completely automated detection of copyrighted works
3. Operates at a level of zero false positives
4. Completely automatic notification of the campus judicial system and/or end user when an infringing activity occurs
5. Graduated response levels, which may include but not limited to user notification levels and/approaches, filtering and/or blocking options which may include varying timeout durations, enabling of tests & quizzes, and other numerous other possible options.
6. Depending on installation location and architecture, ability to detect on-campus and off-campus violations
7. Operates a non-inline, passive device, leveraging a tap-like device to monitor traffic
8. Privacy of content is protected as only infringements of copyrighted works are identified and reported.
9. Enables unfettered communication of all legitimate traffic without violating privacy of the content

## ***2. Performance with Respect to the Requirements Described in the 2007 Workshop Report***

### **2.1 Identifying Infringing Traffic at the Campus Border**

The CopySense Appliance meets all the needs specified in the RFI.

The CopySense Appliance is able to identify copyrighted content with zero false positives, and therefore has no impact on legitimate traffic. (Since the appliance operates efficiently at this level, there is no need to have selectable options based upon a level of false positives.) The appliance can be used to support the accurate identification of the current assignment of IP addresses. In addition, integration with directory services (such as Active Directory and LDAP) are planned that will enable IP independent tracking of users that use multiple internet connections and/or IP addresses.

As a passive device, any failure of the device “fails open”, that is any failure of the appliance has no impact on the flow of legitimate network traffic. As a non-inline device it introduces no additional latency and/or jitter to the network.

The CopySense Graduated Response System enables Network Operations Centers and/or Campus Judicial Systems to configure responses to infringing activities and users. Responses may include user notification and warning levels, requiring quizzes, timeouts on internet access, blocking of infringing streams and other possible approaches. The Graduated Response System is based upon a point accumulation-based system with points assigned to various levels of infringing activities.

Updates and upgrades of the CopySense Appliance, in most cases are automated on a daily basis. These updates and upgrades evolve the technology as new protocols, signatures, modularity’s and other changes that occur in file sharing technologies. The appliance is scalable and may be upgraded to handle most any bandwidth configuration.

Various logging options are configurable which may include retention times. The device has the ability to move logs to other devices. Restrictions in logging are configurable but may disable features like the Graduated Response System and 3-strikes policies that depend upon logging of infringing activities.

## **2.2 Responding to Infringing Traffic at the Campus Border**

The CopySense Appliance meets all the needs specified in the RFI.

The CopySense Appliance Graduated Response System is a point accumulation-based system, which is selectively configurable to perform a range of responses to apply to each university's unique campus policy. This Graduated Response System integrates with existing judicial systems to allow an infinite array of configurable, automated responses to those users committing infringement violations. Various methods of communication with administrators of the Campus Judicial System are also configurable. The system allows flexibility that allows white listing of addresses to disallow monitoring or blocking on selected addresses.

## **2.3 Identifying Infringing Traffic Local to the Campus Network**

The CopySense Appliance meets all the needs specified in the RFI.

If correctly installed within the campus network, the CopySense Appliance is capable of detecting infringing traffic within subnets. Future integration of directory services (ActiveDirectory and LDAP) will allow tracking to the user regardless of the IP address.

See Section 2.1 for additional information.

## **2.4 Responding to Infringing Traffic Local to the Campus Network**

The CopySense Appliance meets all the needs specified in the RFI.

The See Section 2.2 for additional information.

## **2.5 Supporting the Campus Judicial System**

The CopySense Appliance meets all the needs specified in the RFI.

The CopySense Appliance easily automates and integrates using secure, tamper-proof methods with most campus judicial systems. Using standard html, php and/or asp scripts, there is an infinite array of responses and approaches to meet the unique needs of each institution. Meta data associated with what triggered the infringement, the response level (e.g. 3 strikes level), and other related information is available for the automated judicial action. These may include warnings, timeouts, quizzes, and numerous other related actions.

## 2.6 Avoiding Disruption of All Non-infringing Traffic

The CopySense Appliance meets all the needs specified in the RFI.

Operating at a level of zero false positives, non-infringing traffic is not disrupted. As part of the CopySense Appliance Graduated Response System, the system can be setup to account for cases that may be considered permissible under fair use.

## 2.7 Considerations for Purchase and Operations

The CopySense Appliance meets all the needs specified in the RFI.

Audible Magic maintains a standard price list for the various models and configurations of the CopySense Appliance. Pricing consists of three components, the price of the base appliance configuration, the ActiveUpdate Annual Subscription, and if applicable, professional services for those institutions that require customization.

For actual pricing information, please contact Audible Magic directly.

## 3. *Intellectual Property*

Currently, Audible Magic has been issued 4 patents covering the CopySense Appliance and Content Identification. There are 16 other patents pending. A full list of currently awarded patents and abstracts can be found at <http://audiblemagic.com/company/patents.asp>. Below are abstracts of the four awarded patents:

- Copyright Detection and Protection System and Method  
Patent #US 7,363,278 awarded Apr. 22, 2008  
Inventors: Richard Schmelzer and Bryan Pellom

Abstract: A method for detecting against unauthorized transmission of digital works comprises the steps of maintaining a registry of information permitting identification of digital copyrighted works, monitoring a network for transmission of at least one packet-based digital signal, extracting at least one feature from the at least one digital signal, comparing the extracted at least one feature with registry information and applying business rules based on the comparison result.

[Read the full patent US 7,363,278](#) 

- Method and Apparatus for Identifying an Unknown Work  
Patent #US 6,968,337 awarded Nov. 22, 2005  
Inventor: Erling Wold

Abstract: A system for determining an identity of a received work. The system receives audio data for an unknown work. The audio data is divided into segments. The system generates a signature of unknown work from each of the segments. Reduced dimension signatures are then generated at least a portion of the signatures. The reduced dimension signatures are then compared to reduced dimensions signatures of known works that are stored in a database. A list of candidates of know works is generated from the comparison. The signatures of the unknown works are then compared to the signatures of the known works in the list of candidates. The unknown work is then identified as the known work having signature matching within a threshold.

[Read the full patent US 6,968,337](#) 

- Method and Apparatus for Identifying Media Content Presented on a Media Playing Device  
Patent #US 6,834,308 awarded Dec. 21, 2004  
Inventors: Vance Ikezoye and James Schrempp

Abstract: A system and method for identifying media content presented over a media playing device. The media content, such as audio and/or video, is either available digitally or digitally sampled. The media content is sampled to generate a media sample or analytical representation of the media content. The media sample is compared to a collection of sampled (or represented) media content to identify it and to ascertain information related to the sample. This media content-related information is then presented to the user via a display means on the media player. The media play then presents the user specific and related actions that are based upon the information presented and allows the user to directly execute their choice of actions.

[Read the full patent US 6,834,308](#) 

- Method and Article of Manufacture for Content-based Analysis, Storage Retrieval, and Segmentation of Audio Information  
Patent #US 5,918,223 awarded Jun. 29, 1999  
Inventors: Thomas Blum, Douglas Keislar, James Wheaton, Erling Wold

Abstract: A system that performs analysis and comparison of audio data files based upon the content of the data files is presented. The analysis of the audio data produces a set of numeric values (a feature vector) that can be used to classify and rank the similarity

between individual audio files typically stored in a multimedia database or on the World Wide Web. The analysis also facilitates the description of user-defined classes of audio files, based on an analysis of a set of audio files that are members of a user-defined class. The system can find sounds within a longer sound, allowing an audio recording to be automatically segmented into a series of shorter audio segments.

[Read the full patent US 5,918,223](#) 

#### **4. Corporate Characteristics and Resources**

Audible Magic was founded in 1999 as a California corporation and is currently a well-funded privately held company. It currently has less than 50 employees, operates out of multiple locations, which includes Los Gatos, CA; Berkeley, CA; Los Angeles, CA; and the United Kingdom. The company has more than 100 clients, including over 70 public & private universities (e.g. Tulane, Texas A&M, Concorida, and Wittenberg), and over 30 Web 2.0 UGC companies (e.g. Google, MySpace, Microsoft, Nokia, Veoh, and Daily Motion)

#### **5. Pilot Testing**

For institutions that meet specific criteria, demo units may be provided, free of charge, to the institution for pilot testing – generally for a period of two weeks. Scheduling is based upon availability of equipment and an institutions needs. With installations at over 70 colleges and universities, most institutions will find that the CopySense Appliance is already working well in similar environments as their own.

Please contact Audible Magic for more information if a demo unit is desired.

#### **6. Commercial Terms**

Audible Magic sells the CopySense Appliance with standard commercial terms. The CopySense Appliance is purchased as a one-time fee. The ActiveUpdate Subscription is available as a standard annual fee.

Audible Magic does not publically publish its prices list. Please contact Audible Magic for prices of configurations to meet a specific institutions network capacity.

## **7. *Additional Information***

More information about the CopySense Appliance may be found at:

<http://audiblemagic.com/products-services/copysense/>

A list of Audible Magic contacts can be found at:

<http://audiblemagic.com/company/contact.asp>

## **8. *Conflicts of Interest***

Audible Magic is unaware of any potential conflicts of interest regarding this RFI or related institutions.