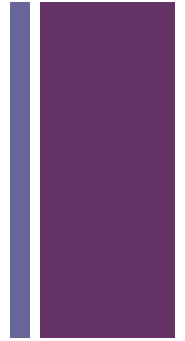




# Managing DMCA Notices

On College & University Networks

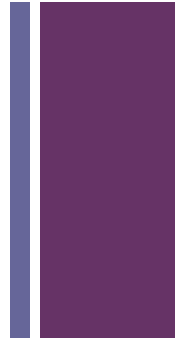


**Presenter:**



**Jay Friedman**  
**VP Marketing**  
**& Customer Support**

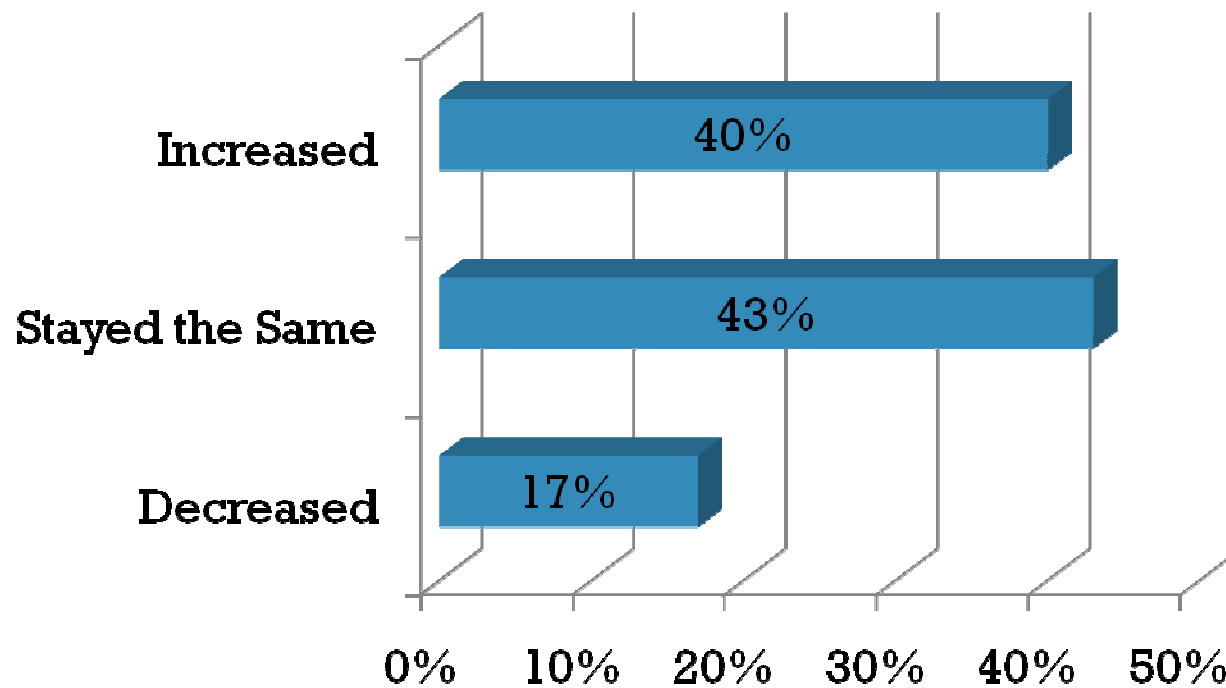
# + Legal Disclaimer



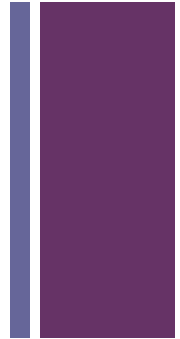
- Please consult your college or university legal counsel for legal advice
- This Webinar is Informational only
- We are not offering legal advice

# + Survey Results

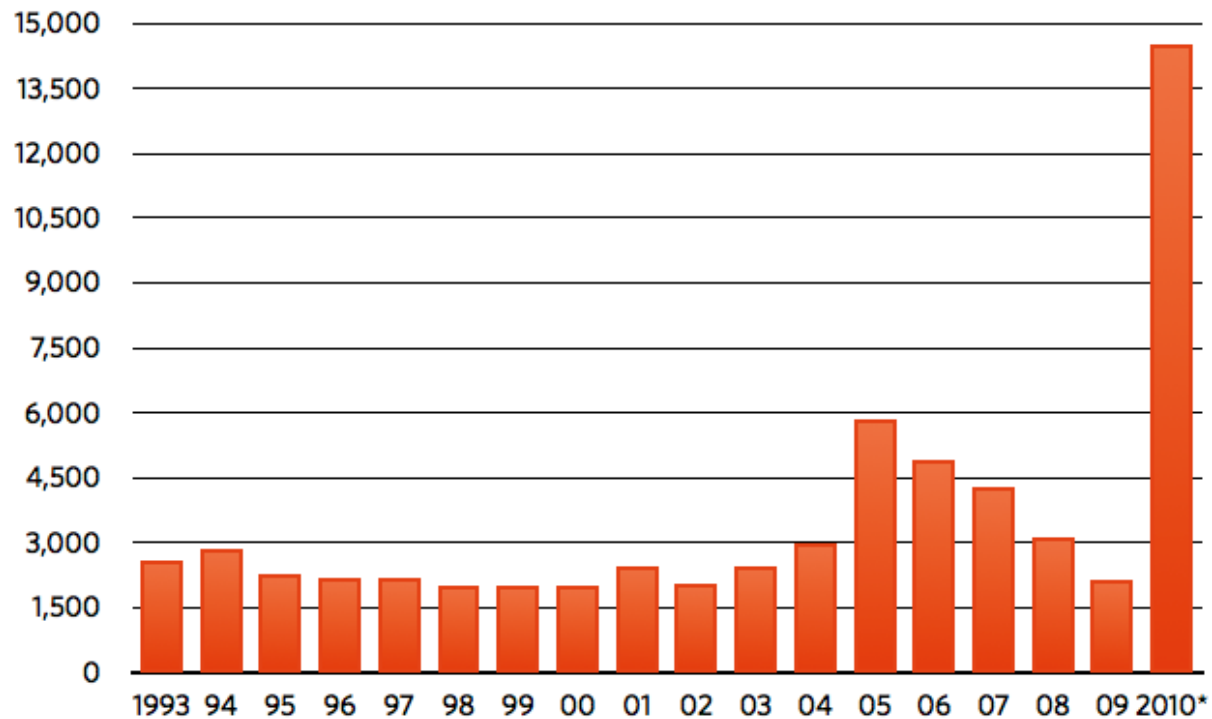
## Number of DMCA take-down notices received compared to one year ago



# + Copyright Lawsuits



**Federal copyright lawsuits by year**

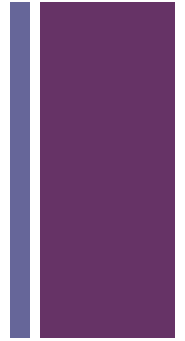


\* Lawsuits filed by US Copyright Group alone



Data source: Administrative Office of the Courts, Wired  
<http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars>

# + Legal Provisions

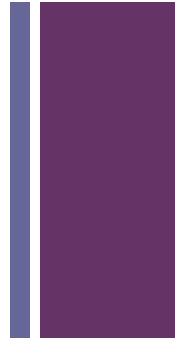


- Digital Millennium Copyright Act (DMCA) of 1998
  - Safe Harbor Provisions – Section §512
  - Responding to DMCA takedown notices
- Higher Education Opportunity Act (HEOA) of 2008
  - Requirements in combating unauthorized distribution of P2P file sharing

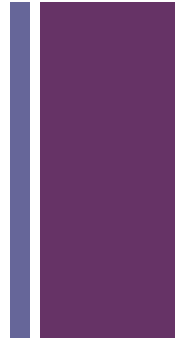
*Note: discuss with your own institutions legal counsel*

# + DMCA Safe Harbor Takedown Notice Provision

- §512(c) – (partial)
  - Upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.
  - **Designated agent.**— The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent.

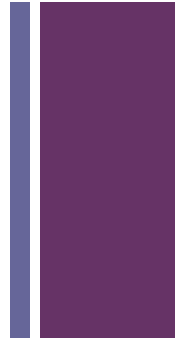


# + Registering Your Agent



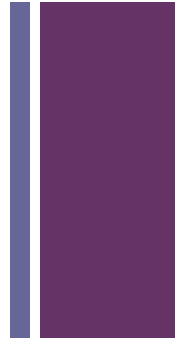
- Less than 30% of all colleges and universities have registered agents
- Download form at <http://www.copyright.gov/onlinesp/>
- More info on the DMCA <http://www.copyright.gov/title17/92chap5.html>

# + Handling DMCA Notices



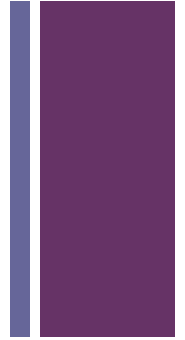
- Every institution must define its own policy and procedures as to its legal obligations:
  - Students, faculty & staff
  - Residential vs. non-residential campuses
  - Volume of notices received annually
  - Honor Codes & Policies
  - Network topology

# + Handling DMCA Notices



- Most institutions have three main components of their policies:
  - Education
  - Communication
  - Compliance & Judicial Affairs

# + Challenges



## ■ Technical Issues

- Identifying the infringing user
- Lack evidence of actual activity
- Unauthenticated networks, esp. wireless networks

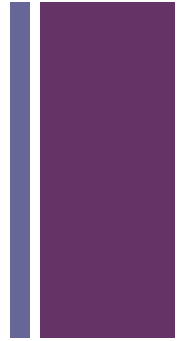
## ■ Budgetary

- Process often requires dedicated staff
- Lack of tools to automate process

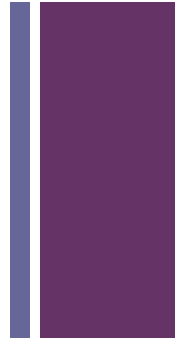
# + Challenges (continued)

## ■ Policy/Enforcement

- Forwarding notice
- Taking action
- Graduated response

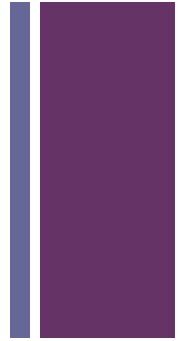


## + Available Tools



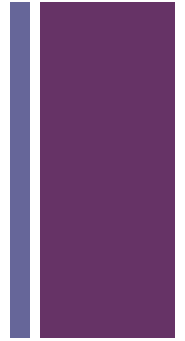
- Mostly home grown tools built by various IT departments
  - Tools are generally unique to the products installed on the campus network
  - Challenge is keeping tools up-to-date as networks change
  - Most tools often still require some manual processing

# + Automated Tool from Audible Magic



- CopySense DMCA Service
  - Fully automates entire process
  - Reads DMCA notices sent by copyright owners
  - Examines relevant log files
  - Identifies user that is the target of the notice
  - Forwards notices to users
  - Able to sanction users via graduated response
  - Integrates with judicial processes

# + A Problem With DMCA Notices



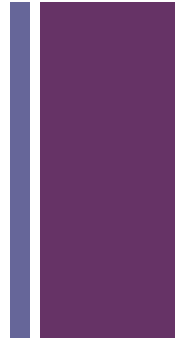
- Notices don't necessarily correlate to the level of illegal activity on campus networks
- With unauthenticated networks it is virtually impossible to identify the offending user
  - Labs, Libraries, Wireless, etc.
- For some law firms, issuing DMCA notices has become a way of making money
- Then there is the HEOA...

# + HEOA Compliance Requirements

- Must provide **annual disclosure** to all students describing copyright law, legal sanctions and campus policies
- Implement a plan that:
  - ✓ **Effectively combats** unauthorized P2P use
  - ✓ Uses at least one **technology-based deterrent**
  - ✓ **Measures** and **reports** effectiveness of your implementation
  - ✓ Includes **periodic reviews** of the plans effectiveness
- Must inform students about **legal alternatives**
- Effective date: **July 1, 2010**

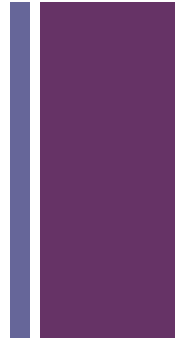
# + Technology-Based Deterrents

- The HEOA requires the use of one or more technologies to combat unauthorized distribution of copyrighted content, which may include but not limited to:
  - ✓ Bandwidth shaping
  - ✓ Traffic monitoring to identify the large bandwidth users
  - ✓ A vigorous program of accepting and responding to DMCA notices.
  - ✓ A variety of commercial products designed to reduce or block illegal file sharing



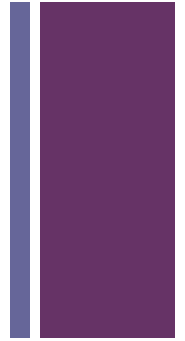
# + Allowances in the Regulations

- Open to interpretation
- Leaves decisions to individual campuses
- Great flexibility in what to implement
- Recognizes that what may work today, may not continue to be effective in the future

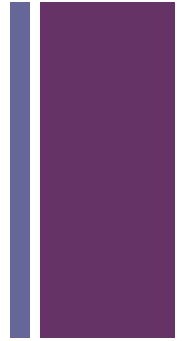


# + Where Does the HEOA Apply on Campus?

- Campus-wide and satellite locations
- Residential and non-residential locations
- Libraries
- Labs/classrooms
- Wireless networks
- Students, faculty, and staff
- Community users



## + What Won't Work

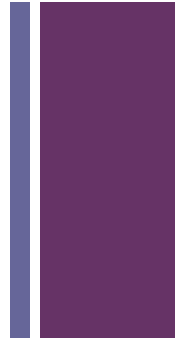


- Assuming the issue will go away
- Assuming that you were already in compliance before the HEOA was implemented
- That you can comply without investing the time & resources
- Thinking all that's required is to write a plan

# + What is the Risk of Non-Compliance?

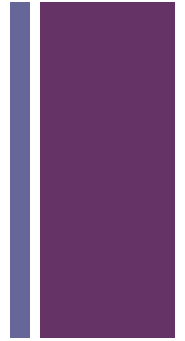
- The regulations do not provide clarity – a commonality with many regulations
- That said:
  - Potential loss of federal funds
  - Boards of Trustees hold a fiduciary responsibility
  - Content owners not content with non-action
  - Expectation of the DoE to enforce
  - Campus image suffers

# + Technological Solutions Using One or More Methods



- Vigorous Response to DMCA Notices
- Educational Solutions
- “Simple” Blocking/Filtering
- Heuristic Identification
- Throttling Devices
- Copyright Detection

# + Is a Vigorous Response to DMCA Notices Enough?

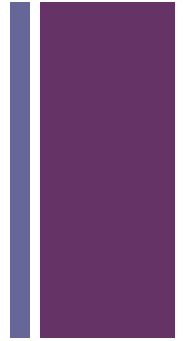


- Only 13% of colleges and universities believe just responding to DMCA notices is all that they need to do
- Pros
  - You may already be doing this today – no additional cost
  - Integrating judicial actions, may be an effective deterrent
- Cons
  - Reactive approach
  - Notices are sent on a very small fraction of the total volume of violations that occur on a network

# + Sample Criteria to Use in Assessment of Technologies

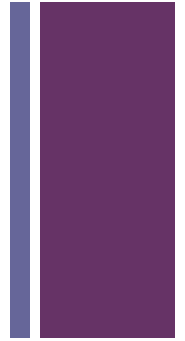
- Reactive vs. proactive approach
- Educational component
- Graduated model
- Integrates with Judicial Process
- Impact on legitimate use
- Addresses P2P & Cyberlockers
- Level of automation
- Security
- User communication
- Addressed encrypted transfers
- Impact on privacy
- Cost plus maintenance
- Adjusts to network topology
- Flexibility
- Ability to circumvent
- Over-blocking
- False positives
- False negatives

# + Educational Technologies



- BAYU – “Be Aware You’re Uploading”
  - Automated tool to notify users via email they are uploading using P2P
- Pros
  - Simple, low-cost approach
  - Provides an educational component
  - Solves problem of users unwittingly enabling uploading on their computer
  - Allows legitimate uses of P2P
- Cons
  - Only solves one part of the problem
  - Does not address problems with cyberlockers
  - Does not address encrypted file sharing

# + “Simple” Blocking & Filtering



## ■ Examples:

- Protocol blocking
- URL filtering

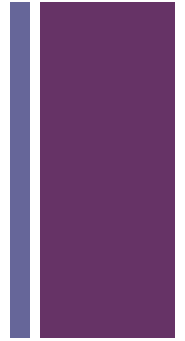
## ■ Pros

- Usually can implement with existing equipment or low cost services
- URL filtering addresses both P2P and cyberlocker activity

## ■ Cons

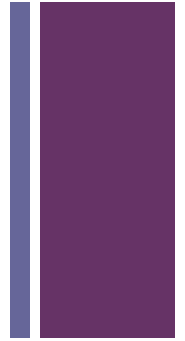
- Susceptible to false positives
- Legitimate uses of P2P will be blocked
- Many P2P clients have methods to circumvent blocking
- Lacks educational component

# + Heuristic Identification



- Example
  - Intrusion Detection Systems
- Pros
  - Multiple use devices
  - “Respects” privacy
- Cons
  - Susceptible to false positives
  - May allow some P2P usage
  - May impact legitimate network activity
  - Lacks educational component
  - Does not address cyberlockers

# + Throttling Devices



## ■ Examples

- Deep Packet Inspection Devices (Allot, Sandvine, etc.)

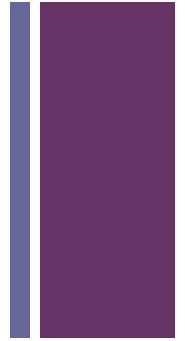
## ■ Pros

- Multiple use devices, including Quality of Service management
- Limits use related to inappropriate activities

## ■ Cos

- Lacks educational model
- Unauthorized P2P and cyberlocker activity still exists on network

# + Copyright Detection Devices



## ■ Example

- Audible Magic's CopySense Network Appliance

## ■ Pros

- Specifically targets in real-time theft of copyrighted works
- Fully automated educational and graduated sanction model
- Targets both encrypted and unencrypted traffic
- Does not impact legitimate network activity
- Address both P2P and cyberlocker usage
- No false positives

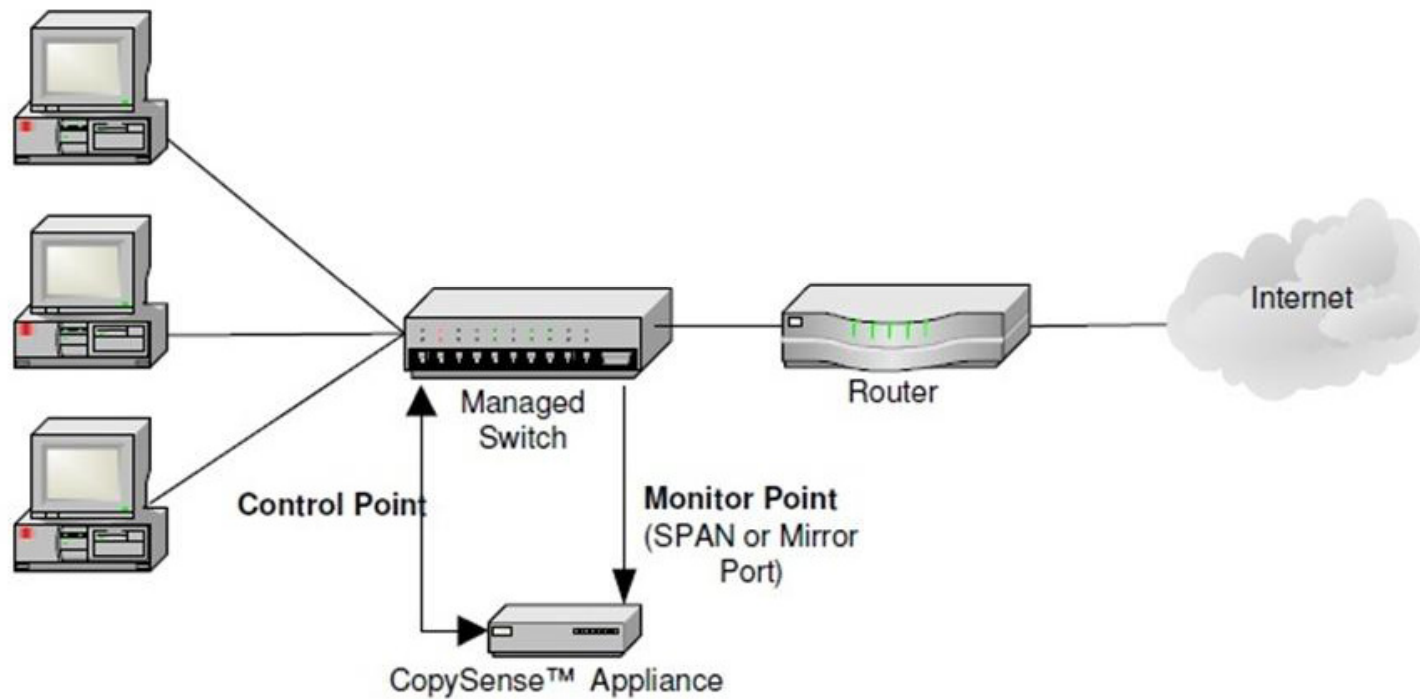
## ■ Cons

- Deep packet inspection (knowledge only of copyrighted works)

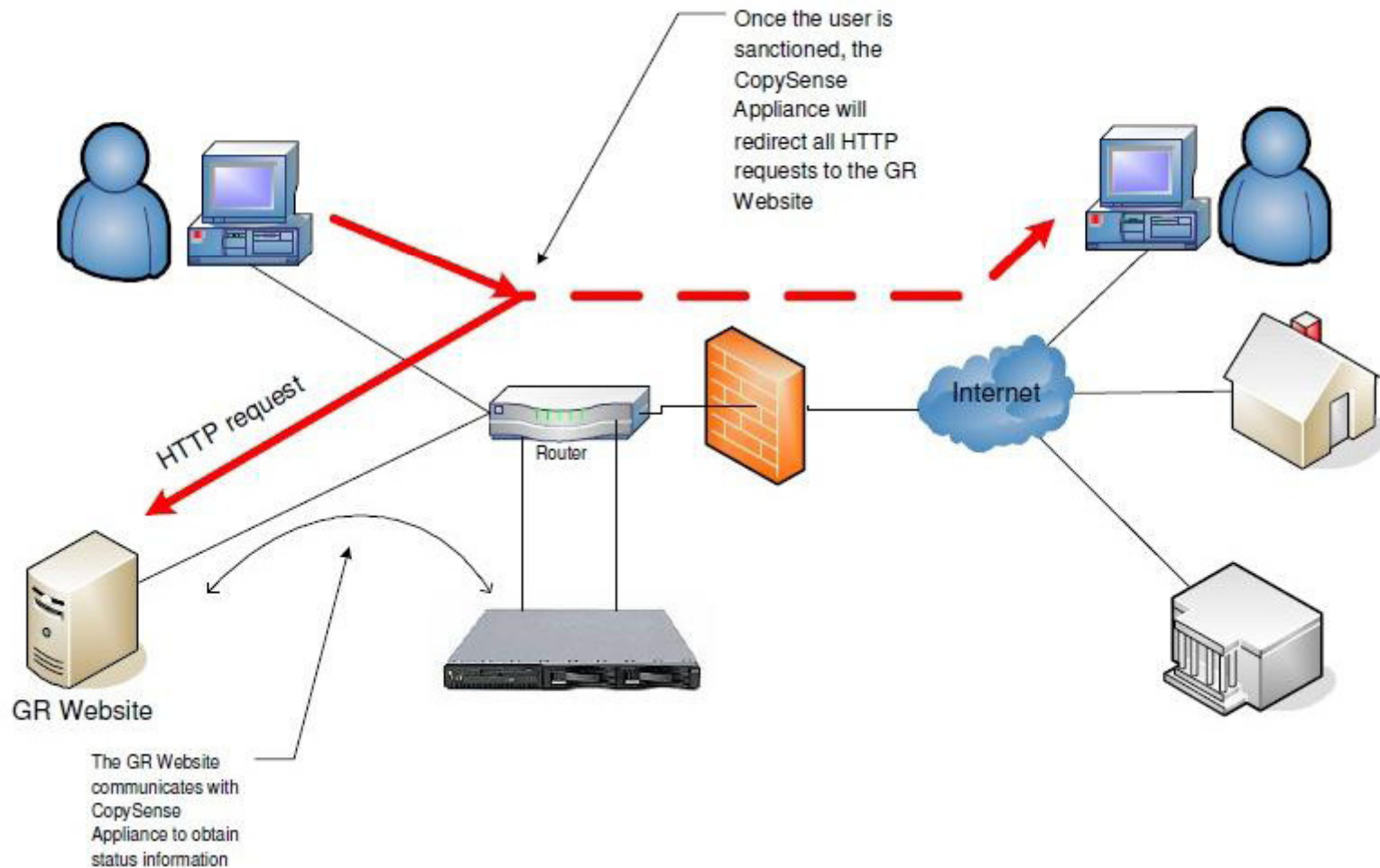
## + How Detection Works with the CopySense Network Appliance

- A digital fingerprint is extracted of the audio and video images of the unknown content
- The unknown digital fingerprint is matched to a master fingerprint database of over 11 million tracks & videos registered by content owners
- Only identifies **unauthorized** distribution of works
- Considered to be the industry's “gold” standard

# + Simple Non-Inline Approach with the CopySense Appliance

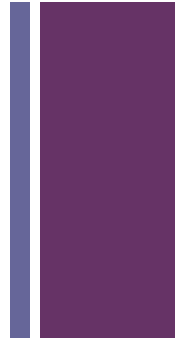


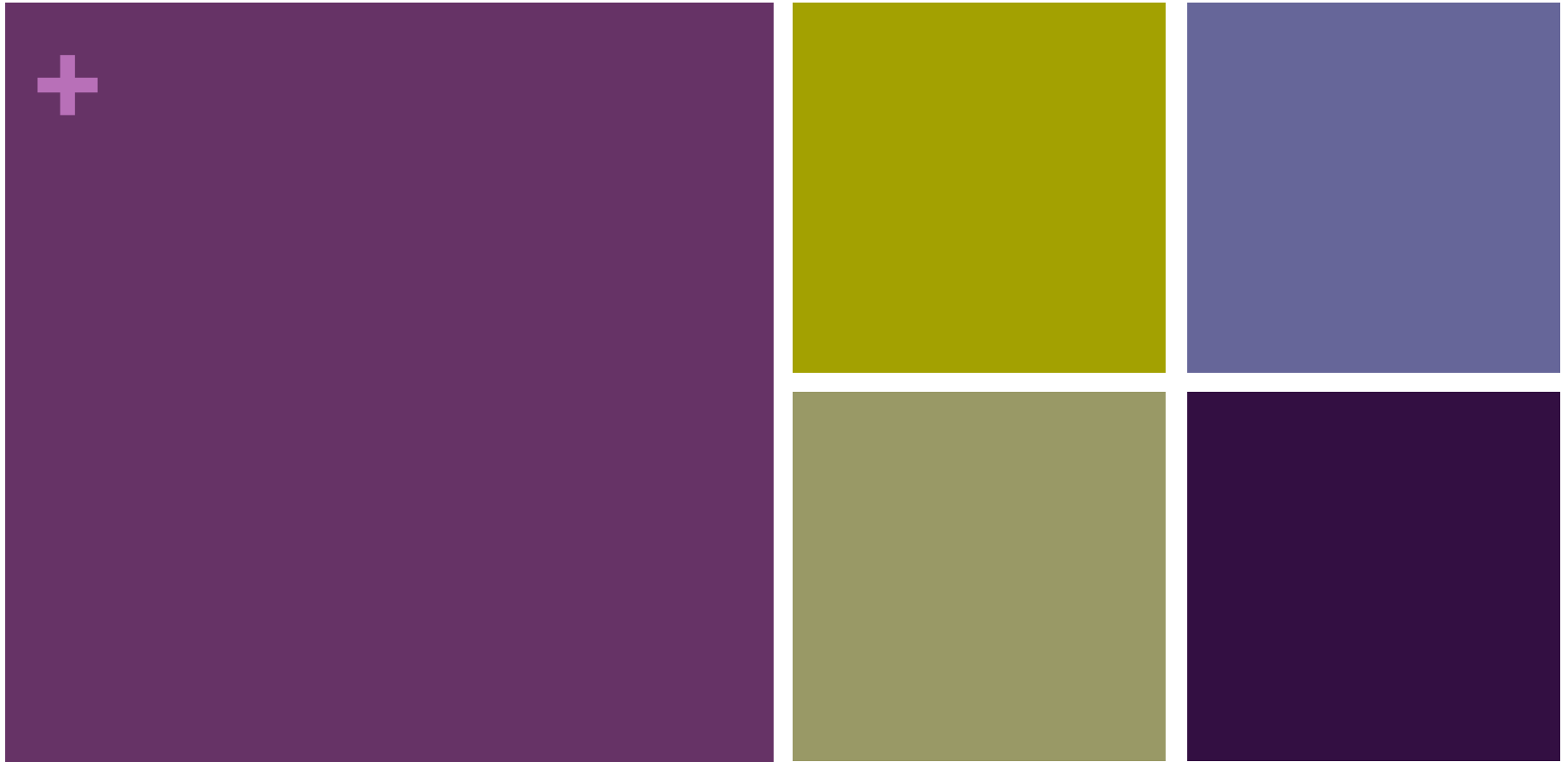
# + Graduated Response – Web Redirect or Email Communication



# + Resource Information

- Audible Magic
  - Email: [info@audiblemagic.com](mailto:info@audiblemagic.com)
  - Website: <http://audiblemagic.com/HEOA>
    - Resource Links
    - This webinar
- Educause





Thank You!

