Global File Registry
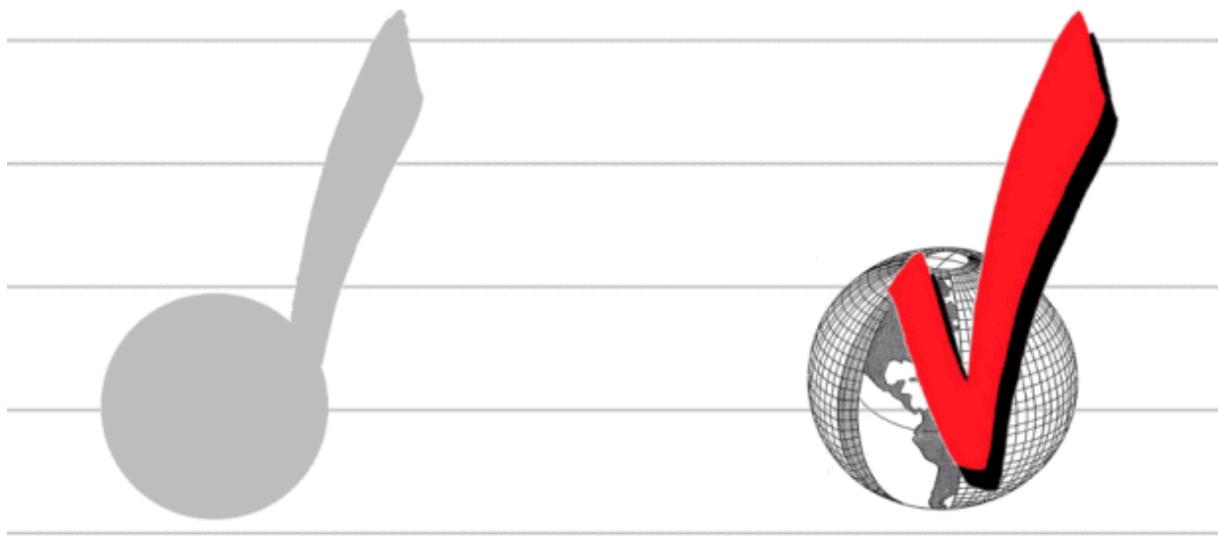
TECHNICAL WHITE PAPER

© GLOBAL FILE REGISTRY

STRICTLY CONFIDENTIAL

Draft 1 – 26 May 2006

CONTENTS

BACKGROUND

2006 – The year that DMCA take-downs take off

It's been 7 years since the DMCA take-down provisions became law in 1998. For most of those years the number of DMCA take-down issued per month has been negligible – certainly not enough to warrant the creation of an automated Global File Registry, as proposed here.

The reason for so few DMCA notices being issued during this period is that DMCA-capable web search engines such as Google and Yahoo simply didn't index audio or video content – i.e. these site search engines provided consumers with no way to search for "Battlestar Galactica.AVI".

Conversely, P2P networks such as Limewire, Kazaa and eDonkey, which do allow users to search for MP3 and AVI files, had no means of acting on a DMCA takedown notice, as there was no way for the operators of those networks to 'take down' selected files from their networks.

Between the web search engine (which had few direct links to infringing content) and P2P networks (which had no way to remove infringing content), there was simply no 'market' for DMCA take-down notices. As a result, the number of DMCA take-down notices issued per month was minimal – on the order of hundreds per month.

However, the emergence of three new trends is set to change this – explosively:

1. Major search engines now search audio and video files
   Major search engines are introducing services to specifically search for, and offer links to, audio and video content. For instance, Google's just-introduced Music Search allows users to search for audio content by artist, album or track name.

   The search engine operators are relying on the DMCA safe-harbor provisions to protect them from liability for indexing infringing files. Specifically, they are relying on content owners to notify them of infringing content and issue DMCA take-down notices for each infringing file. The. the burden of detecting infringing content and notifying the search engine provider falls upon the content owner as never before. In the absence of the content owner diligently checking every web search engine for infringing copies of their works, the search engine operator has no obligation to identify or remove such content.

   Given that Google, Yahoo and MSN each have on the order of 10 BILLION web pages in their indexes, the potential for unintentional indexing of infringing content is huge. For instance, if search engines index just 1% as many MP3 and AVI files as they currently index HTML pages, that means potentially 100 MILLION MP3 and AVI files coming online over the coming months in each of the major search engines.

   Unless content owners take steps to prepare for it now, the explosion in the availability of audio and video content will catch them without a take-down solution in place, and millions of infringing tracks could be available as search results for weeks or months without the content owner being aware of it and issuing the necessary take-down notices.

2. Rise of Social Networking web sites
   Social Networking web sites (also loosely known as Web 2.0 services) allow users to create their own online spaces, link to each other, add files to their spaces, add RSS feeds to each other's content, 'mash up' and remix existing content, and more.

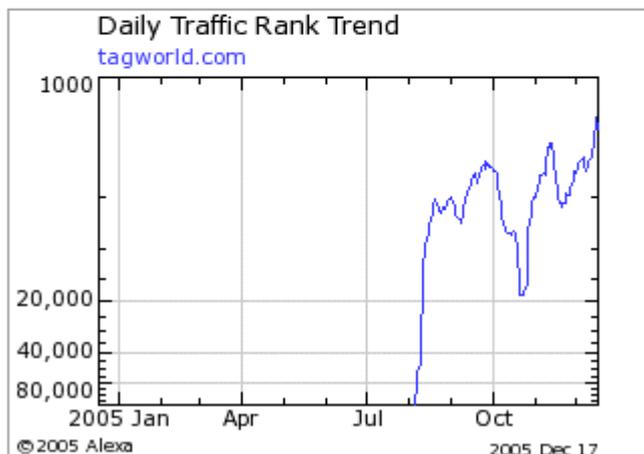   The growth in social networking sites in just 12 months has been spectacular:

MySpace (recently acquired by News Corp) allows users to create their own 'spaces', to which they can add audio and video files, invite friends, etc.

MySpace is now the 12th most popular web site by unique users, and has more page views than Google.


del.icio.us (recently acquired by Yahoo) is a social tagging site which allows users to recommend sites to each other, link to socially-nominated cool sites, subscribe to RSS feeds from favorite sites, and more.

Tagworld, launched only a few months ago, has rapidly climbed to become the 1000th most popular web site.

The rapid growth in social networking services can be clearly seen in the graph below, which compares the internet ranking of Apple (including iTunes) and the Warner Bros. web site (including the wbmovies.com entertainment site) with del.icio.us, one of the new Web 2.0 social networking sites:

Daily Traffic Rank Trend

© 2005 Alexa   2005 Dec 17
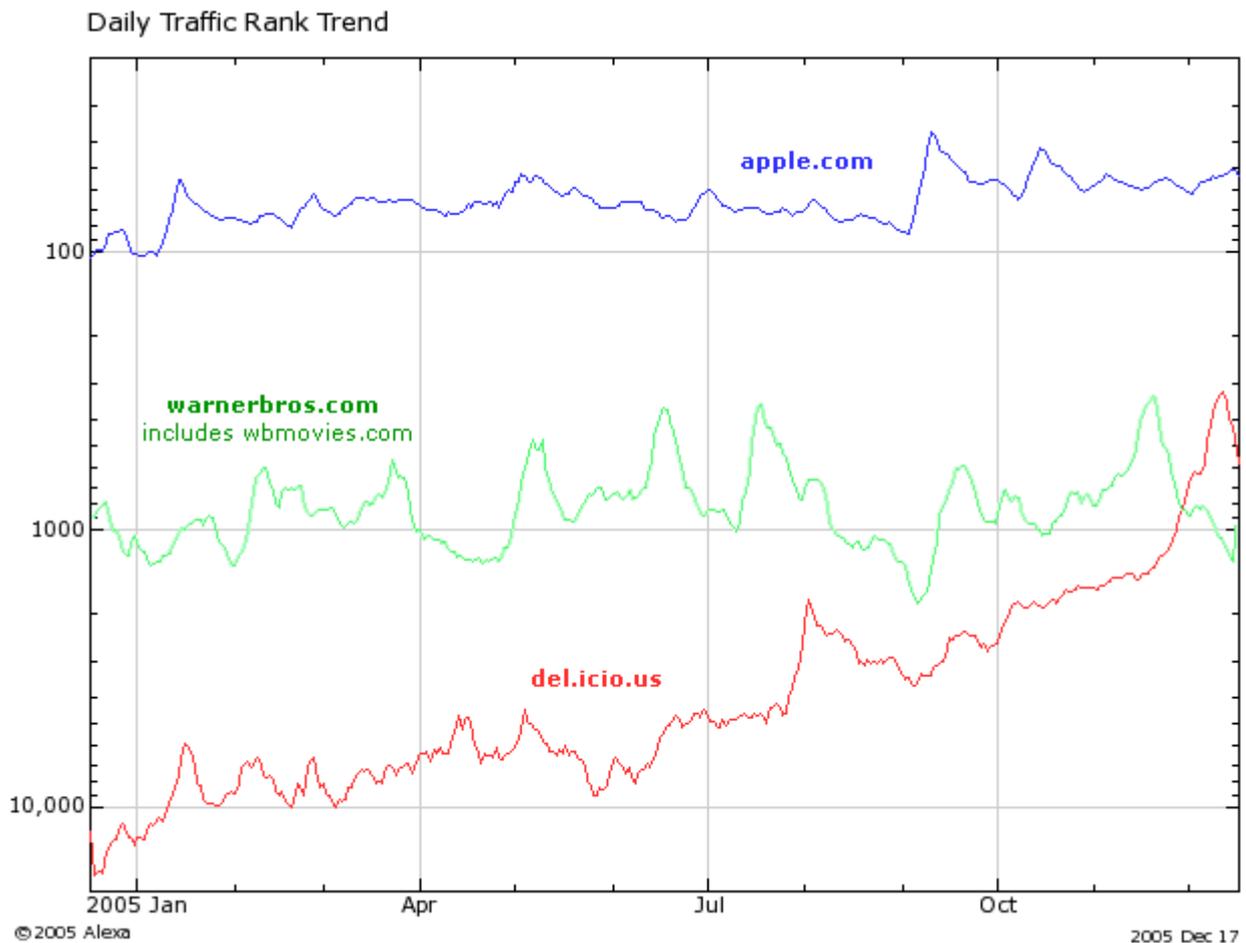
[a rank of 100 means that site is the 100th most popular web site]

The rise in social networking sites has been so rapid that their effects on both traditional corporate entertainment sites and existing P2P services has yet to be fully understood. However, it's likely that they're cannibalizing users from both 'legal' entertainment sites and P2P services, dropping users into public and private spaces of their own making – with those spaces potentially containing a variety of infringing and non-infringing material.

Like web search engine operators, the operators of these social networking sites are relying on the safe-harbor provisions of the DMCA to protect them from liability for any infringing content found on their sites. Again, this puts a new and onerous burden on content owners to diligently patrol those spaces and serve DMCA take-down notices to specific items of infringing content found in those spaces.

3. **P2P operators begin to embrace DMCA**
    Some P2P operators are beginning to engineer new classes of P2P services that provide them with safe harbor, thanks to the DMCA's liability exclusion provisions for ISPs, search engines and web sites who provide a DMCA take-down facility.

    The recent US Supreme Court rulings changed the P2P landscape. One can assume that there are new classes of P2P services in development that will, for the first time, provide the P2P operators with enough network control to be able to take down infringing content, if notified to do so by a content owner.

    Bram Cohen recently became the first P2P operator to offer DMCA take-down, on the bittorrent.com site, which operates as a search engine for BitTorrent links.

    The bittorrent.com web site is, being a web site, fully centralized and hence it's easy for the operator to implement a DMCA take-down system.

    Existing P2P services are for the most part fully decentralized, and impossible to control in this way. While some P2P operators would be keen to keep things this way, and indeed would likely be working to increase user anonymity in their networks, add encryption layers to prevent eavesdropping on network traffic by content owners, etc., it's reasonable to envisage that the more commercially astute P2P network operators may be looking to do just the opposite, giving their services the same legal status as any of the major web search engines by adding the technological controls to be able to offer a DMCA take-down service.

    Once P2P services offer such a take-down provision, the burden of identification and notification will again be on the content owner, who will have to endlessly patrol these networks looking for infringing copies of their content, then issuing take-down notices for each infringing file – an onerous task.

Need for a central content registry

With the onus on the content owner to issue DMCA take-down notices to sites and services that are hosting infringing content, each content owner is going to have to trawl thousands of web sites and issue take-down notices to them on an individual basis.

Likewise, each web site is going to have to deal with take-down notices coming in from dozens or hundreds of content owners.

The situation will look something like this:
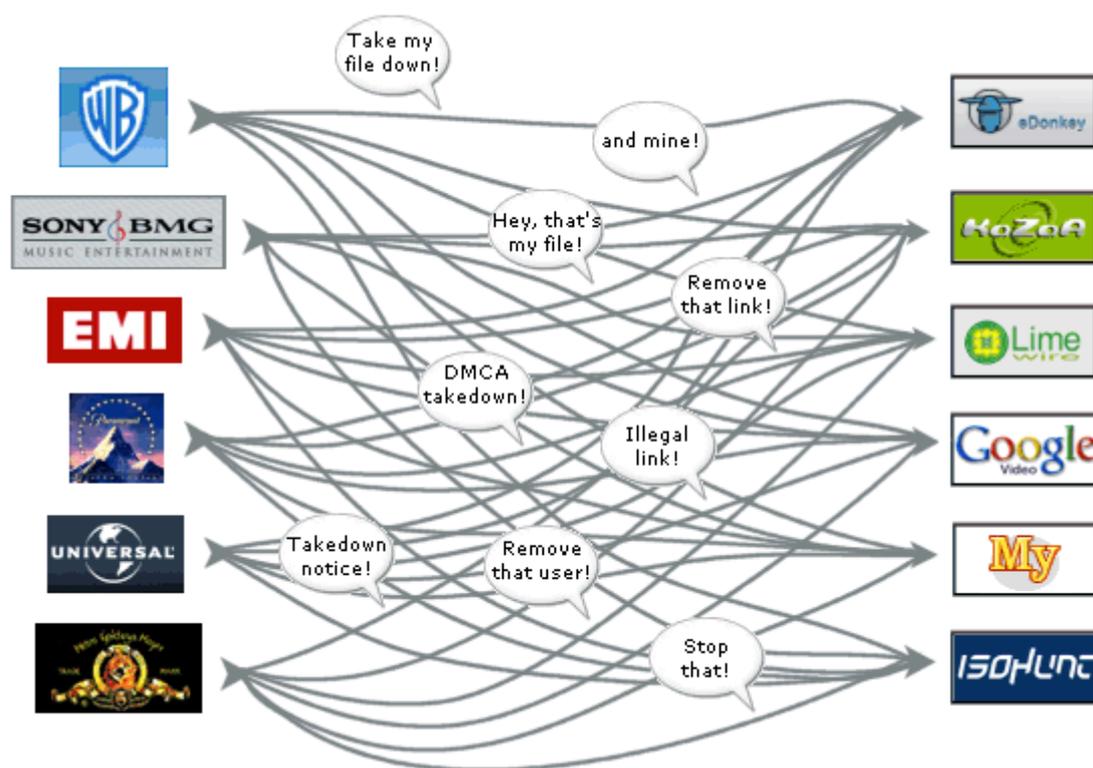
Now multiply the image above by a thousand to account for the thousands of web sites that each content owner will need to have a relationship with.

Each of those thousands of web sites will need to verify that the content owner who has supplied the DMCA take-down notice is authorized to do so – i.e. is the owner or licensee of that content, and as a result each content owner is going to have to prove their credentials to each and every site for each new piece of content that they want to have removed from that site.

It's clearly an unworkable situation.

Global File Registry, supported by Altnet's TrueNames patent, intends to provide a solution.

INTRODUCING... GLOBAL FILE REGISTRY

Global File Registry brings order to the chaos. Instead of each content owner needing to have a one-to-one relationship with each web site and P2P service, content partners need just a single relationship with globalfileregistry.com, and we take care of the rest.
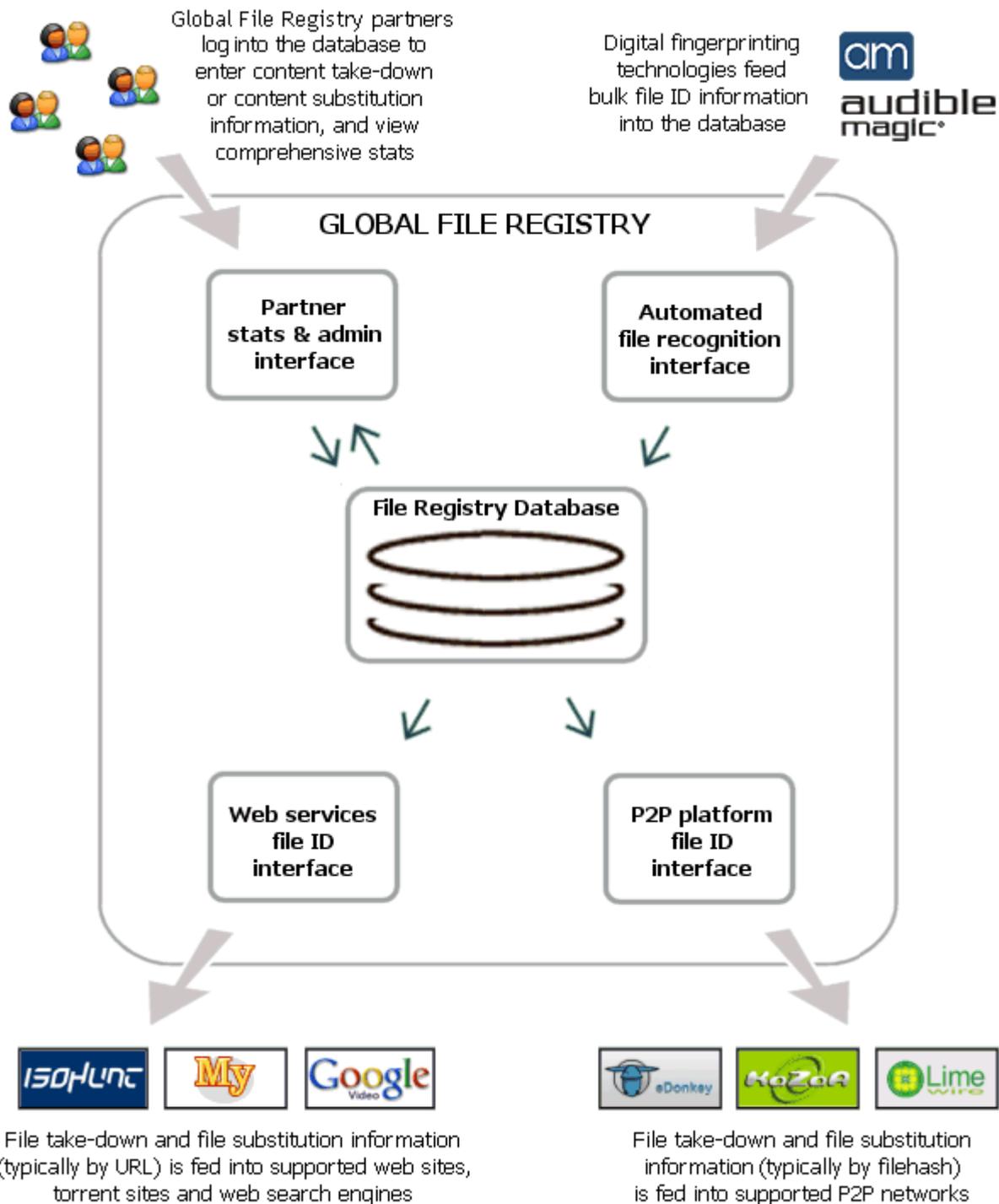
How it Works

Here's an overview of the main elements which make up GlobalFileRegistry:

- GlobalFileRegistry provides a centralized database that contains the unique identifiers of millions of infringing files captured and collated on behalf of multiple content owners.

- Each content owner can provide their employees with secure authenticated login to the GlobalFileRegistry database via a BackOffice interface (depicted at the top left of the above image). Content owners can log in to quickly register and assert that a particular content item is owned by them and should be taken down on a particular search engine, torrent site or P2P network.

- Given the huge catalog of licensed content, an automated batch process will be available to register ownership of thousands of unique identifiers (representing content items) at one time. Instead of employees needing to manually type in the unique identifiers for thousands of files, content owners can connect their databases, or the databases of companies who they already employ to patrol search engines and P2P networks, directly to the GlobalFileRegistry database.

  To facilitate this, GlobalFileRegistry provides a web services interface (top right of the above image) which allows existing or new databases to batch input thousands or millions of file identifiers directly into the GlobalFileRegistry database.

- GlobalFileRegistry provides a web services interface to supported web search engines, torrent sites and social networking sites (bottom left of the above image) – this is the channel by which take-down notices are automatically served into those sites. Web sites and search engines will use this take-down web services interface to periodically receive a feed of the latest take-down notices from GlobalFileRegistry, then remove those files from their search databases.

- P2P networks work in a very different way to web sites and won't be able to make use of the web services take-down method applicable to web sites and search engines. GlobalFileRegistry supports P2P networks via a series of dedicated P2P connectors.

  Each supported P2P network has a 'connector' (depicted at the bottom right of the above image) which allows the information in the GlobalFileRegistry database to propagate to nodes on that P2P network. Files marked with take-down notices in the GlobalFileRegistry database simply disappear from those P2P networks, and don't even show up as search results.

  Through its P2P knowledge and experience, GlobalFileRegistry is uniquely able to build these connectors and 'publish' take-down information into supported P2P networks.

- Content owners can log into the GlobalFileRegistry BackOffice to view comprehensive file and network statistics showing the number of take-downs issued to each search engine and P2P network, view an audit trail showing which of their employees logged in and issued take-down notices, and more.

The elements outlined above will now be described in detail over the following pages.

BACKOFFICE: TOP-LEVEL NAVIGATION

When entering GlobalFileRegistry's BackOffice web interface, the user is presented with the following list of available options:

Menu option	Description
Files and Users	
Add/Edit blocked files	This area allows content owners to issue a take-down or
Add/Edit blocked users	put-back notice for a specific file or user
Traffic	
- Download Summary	This section allows partners to view the number of
- Downloads by File	download requests, take-downs, etc. for specific file(s)
- Downloads by Network	in total or for a specific web site or P2P network
Revenue	
- Sales Summary	In addition to taking down infringing content,
- Sales by File	GlobalFileRegistry can substitute infringing files with paid
- Sales by Network	licensed versions – view here the sales revenue for those files
Administration	
- Add/Edit Member	This section is used by GlobalFileRegistry personnel to
- Add/Edit Partner	configure new content providers ("Partners"), their
- Add/Edit Network	employees ("Members") and supported take-down networks
Auditing	
- Member activity	This section provides GlobalFileRegistry personnel and
- Takedown log	partners with a means to audit the take-down and put-back
- Put-Back log	requests that have been entered into the system
Network connectors	
- Publish to P2P network	This section allows take-down information to be 'exported' to
- Publish to file	supported P2P networks and external databases
Help	
- Online documentation	BackOffice members can access customer support and help
- Customer support	information here

These menu options are described in detail over the following pages.

BACKOFFICE: TAKE-DOWN FUNCTIONS

Searching and browsing Take-Down Campaigns

To allow the huge number of files in the GlobalFileRegistry to be accurately and efficiently managed, related files can be conveniently grouped in to Campaigns.

- A partner (in the examples below we'll use the hypothetical partner "33rd Street Records") can create as many campaigns as they wish.
- The partner can add any number of files to each campaign.
- A campaign can be thought of as being equivalent to a directory or folder in Windows – it's a convenient place to group similar files.
- For music files, the partner may wish to create one campaign for each artist, or one campaign for each album – whatever is most convenient.
- For video files, the partner may choose to create one campaign for a TV series, then put all the shows the series into that campaign.

The image below shows partner 33rd Street Records being able to
- search through their campaigns
  (e.g. they can easily display all campaigns that contain a particular file)
- browse through the list of all their campaigns
- create a new campaign

To create a new set of Blocked Files – i.e. to block one or more files from appearing on one or more networks supported by GlobalFileRegistry – click the New Campaign button, then keep reading…

Creating a Take-Down Campaign

Creating a new campaign is easy: Start by giving your campaign a Campaign Name and selecting the dates when it should be live:

- Outside of your selected Campaign Dates, GlobalFileRegistry will automatically expire your campaign and allow your content to be available on web sites & P2P networks.

- GlobalFileRegistry will automatically register the name of the person who created or lat modified the campaign ("Bob Smith" in the above screenshot) providing for full audit trail logging of take-down and put-back notices.

You can now add Title and other descriptive information to your campaign – this is useful in later identifying that campaign in Traffic and Sales reports:

Adding Files to a Take-Down Campaign

Having created a campaign, you can now begin adding files to your campaign.
Start by clicking the Files tab:

- Click Add File to create a new blocked file entry in the GlobalFileRegistry database.

- To edit an existing entry (to, for instance, add extra filehash identifiers for that file - see below for details) just click on that file entry.

- Each file can be quickly and easily Enabled or Disabled - "Enabled" means that GlobalFileRegistry will begin issuing take-down instructions for this file.

- A View Stats link allows you to navigate in one click to the Traffic report for that file.

Specifying Take-Down File Attributes

Having created a new file entry, you can now begin entering or editing the attributes and take-down options for that file:

If the file is to be taken down on, say, the Gnutella network, then you would select the Gnutella network option, then enter one or more Gnutella-specific file identifiers. For instance, the Gnutella network identifies files by a 128bit filehash, so you would enter the filehash (or filehashes) of each infringing version of the file that has been identified on the Gnutella network and is to be taken down.

For networks such as social networking web sites which support user groups and spaces, you may also enter one or more Space Identifiers for each File Identifier. This is explained in more detail on the next page.

Replacing infringing files with DRM licensed versions
Finally, instead of just taking down infringing files, it's possible (on networks which support such functionality) to replace the file with a DRM licensed version. For instance, if User A shares out a ripped copy of Battlestar Galactica, then GlobalFileRegistry may be able to replace its filehash with the hash and fallback URL of a paid licensed version of that file. When User B now tries to download the file, he/she will download the licensed version instead of the ripped version. When User B plays the file, a popup DRM window will appear, asking the user to purchase the file and/or automatically making the file available to the user if they have subscribed to an appropriate subscription plan.

About File and Space Identifiers...

Adding a file entry won't on its own do anything to remove that file from supported networks – you need to specify one or more unique identifiers for that file. Supported networks use this unique identifier to identify the file when it appears on that network.

The unique identifier is therefore different, or potentially different, for each supported network. For instance, P2P networks usually treat a file as being different to another file if it has a different filehash, and therefore for P2P networks the unique identifier is typically a filehash. On the other hand, a web server thinks in terms of URLs, so for web sites the unique identifier would typically be a URL.

The table below lists the unique identifiers typically associated with each of the various classes of networks supported by GlobalFileRegistry:

Network	Unique identifier type	Additional qualifiers
BitTorrent	128bit filehash	---
Gnutella	128bit filehash	---
FastTrack	160bit filehash	---
Web site	URL	---
Web search engine	URL, filehash or file ID	user group/space name
Social Networking site	URL, filehash or file ID	user group/space name

In addition to requiring a unique identifier such as a File ID, newer types of social networking web sites may require additional qualifiers to locate the file within a particular user group or a particular collaborative space.

For instance, if a particular file is to be removed from The Anarchy Collective, a hypothetical collaborative workspace on a social networking site, then that site would need to be told both a unique identifier for that file as well as the name of the collaborative workspace which it needs to be removed from.

GlobalFileRegistry's ability to support unique identifiers in a number of different formats plus additional 'Space' qualifiers provides compatibility with the greatest number of existing network types, as well as ensuring compatibility with the growing list of new-style social networking sites and applications.

The DMCA take-down provisions allow for users who frequently post infringing content to have their accounts revoked. Accordingly, GlobalFileRegistry provides for a means to take down such frequently-infringing users on networks that support such functionality.

The process of taking down a user account is similar to taking down a file, shown above, but instead of entering a file identifier (filehash, etc.) one enters an identifier for that user appropriate to the P2P network or web site on which the user is to be blocked or their account is to be disabled:

Put-Back functions:	Restoring blocked files and users

The DMCA take-down provisions require that incorrectly taken down files and users be able to be restored. Accordingly, GlobalFileRegistry provides facilities for easily 'putting back' any files or users that may have been incorrectly removed.

To restore a taken-down file or user, simply uncheck the checkbox that appears next to each File Identifier, Space Identifier and User Identifier in the GlobalFileRegistry BackOffice interface:

GlobalFileRegistry will now
a) cease issuing take-down notices for this identifier, and
b) begin issuing Put-Back notices to networks that support such functionality – this allows files that have been removed from search index databases to be restored and made available again for searching.

BACKOFFICE: ADMIN FUNCTIONS

Admin functions	Adding a Member

This section of BackOffice is only available to GlobalFileRegistry personnel, but it's instructive to provide here an overview of some of the available functionality.

Let's first examine the process of creating a new Member – that's a person who is allowed to log into GlobalFileRegistry BackOffice to issue take-down notices on behalf of one or more content owners, view stats and take-down audit information, etc.

In the example below, we're setting up Bob Smith as a Content Owner – this allows him to act on behalf of a content company such as 33rd Street Records, our hypothetical content partner – and to enter take-down notices and view stats for that partner:

Instead of setting up Bob as a Content Owner, we could instead have given him:
• Accounting/Auditing permissions, which would allow him to view stats for the relevant partners but not issue take-down notices, or
• Network Operator permissions, which would allow him to view stats across all content partners but limited to a particular network (e.g. FastTrack), or
• Administrator permissions, which would allow Bob full access to all BackOffice functions, including allowing him to create new Members.

"Partners" are companies who own content. For instance, our hypothetical 33rd Street Records is a company who wishes to use GlobalFileRegistry's services to remove infringing copies of their content from supported networks, and hence they would be set up as a Partner in the GlobalFileRegistry database.

33rd Street Records would now be configured as a BackOffice Partner:

We can now provide Members (such as Bob Smith in the above examples) with permissions to create Take-Down Campaigns for this partner, and this partner's take-down stats will now become available in BackOffice traffic and auditing reports.

Additionally, by assigning a Password to a partner account, it becomes possible for that partner's database to connect directly to the GlobalFileRegistry database using GlobalFileRegistry's Web Services interface. This allows the content partner to directly issue take-down notices from their database into the GlobalFileRegistry database, with no manual intervention needed.

For instance, 33rd Street Records could connect their CD catalog database directly to the GlobalFileRegistry database. Each time 33rd Street Records release a new CD, their database can automatically create a Take-Down Campaign for all songs on that CD directly in the GlobalFileRegistry database. In order for those files to be taken down on supported networks it's still necessary to enter take-down File Identifiers for each file to be taken down, but by creating the framework of Take-Down Campaigns for all their content it become faster and easier for individuals or automated network patrollers to post unique identifiers for that content as infringing copies are discovered on supported networks.

BACKOFFICE: REPORTS

GlobalFileRegistry provides a comprehensive range of reports which allow content owners and network operators to monitor and audit take-down activity. The sections below provide a brief overview of the available functionality.

Reports	Traffic Reports

Traffic Reports show the daily/weekly/monthly number of take-down notices issued for each campaign, file and network, plus distribution of take-down notices by network, etc.
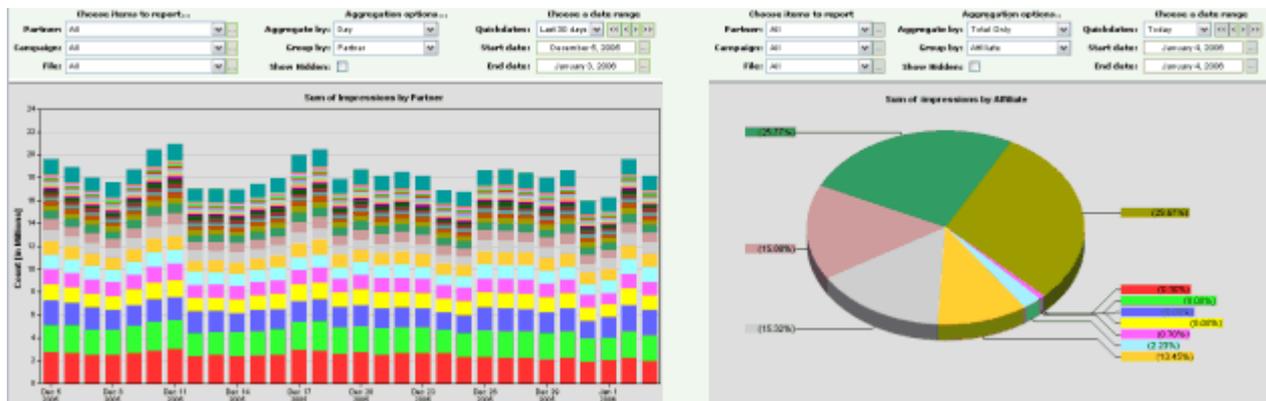
Reports	Take-Down Reports

Take-Down Reports provide an audit trail showing when each take-down and put-back notice was issued to each supported network.

A sophisticated database search filter makes it quick and easy to find out when a take-down or put-back notice was issued for a specified file, file identifier, user, etc., for any given supported network – essential for sorting out any disputes that may arise as to whether a take-down notice was issued and was propagated to a particular supported network.

Reports	Member Activity

Member Activity reports provide an audit trail listing the BackOffice activity of each Member who has BackOffice access. For instance, if Bob Smith creates a Take-Down Campaign on behalf of 33rd Street Records and adds 10 files to that campaign, then each of those actions will be logged in his Member Activity report. System auditors can quickly trace the source of any particular take-down or put-back notice, pinpoint the individual responsible for issuing that take-down notice, the time that they logged in to BackOffice, etc.