



Comment Number: OL-100058
Received: 12/31/2004 3:13:07 AM
Submitted As: CW Web Form
Organization: RazorPop
Commenter: Marc Freedman
Agency: Federal Trade Commission
Rule: Notice Announcing Public Workshop and Requesting Public Comment and Participation
Docket ID: Not yet available
Attachment: [vigilante-ftp.htm](#)
Attachment: [vigilante-ftp.htm](#)

Comments:

RIAA Vigilante Justice

This article builds on previous [blog](#) entries

RIAA (The Recording Industry Association of America) openly acknowledges distributing bogus files to deter alleged copyright infringement on the P2P file sharing networks. This is a significant activity as a presentation at the FTC workshop indicated that up to 50% of certain music files are such bogus files. This consumer risk affects not only the user downloading the bogus file, but also other P2P users across the network. The entertainment industry believes their action is justified. This article looks at the ethical and legal issues.

A SIMILAR CASE - ATTACKING SPAMMERS

Spam, like copyright infringement, is a significant issue. Lycos Europe started combatting spammers by [distributing software](#) that would attack their Internet servers. The intent was not that this would be a directly harmful act like a true Denial of Service attack that floods the server with requests until the server crashes. Instead this was a kinder, gentler approach. It would be a nuisance. The software would send a lot of web server requests, but not enough to crash a server.

After Lycos proposed their plan there was a [firestorm](#) of [controversy](#). Lycos [canceled the attack](#) due to the public outcry.



This article will not go into detail on the ethics of the Lycos attack. For that I highly recommend Carlton Vogt's excellent [Enterprise Ethics](#) newsletter. His article "The Case Against Vigilantism: Is it ethical to use unethical tactics against someone you consider unethical?" persuasively and clearly answers 'no'. You'll need to subscribe to read it.

Nobody questions the ideal that users should be safe from spam, or that content owners have a right to secure their property. But having the right to protect yourself is not the same as having the right to attack another party. The United States has a clear justice system. The fundamental problem in the Lycos case is that they served as judge and jury. Their distributing attack software was an act of vigilante justice. Ethically it's wrong to take matters in your own hands without due process and without a trial, no matter the intent.

What wasn't addressed in the Ethics article or in the Lycos because the software was quickly pulled was the huge potential for civil and financial liability. Legally Lycos could have been held responsible for any damages as a result of the attacks.

WHAT ARE BOGUS FILES?

Bogus files look legitimate. File names correspond to popular songs and movies. A bogus file can have a legitimate hash code (only the bogus file has that unique hash code) or a falsified or spoofed hash code (the bogus file shares the hash code with a suspected copyright infringing file). When bogus files are played the user doesn't get what he expects. The file may contain silence, noise, or simply not work.

THE RATIONALE AND EFFECT OF BOGUS FILES

A copyright owner makes it harder for users to obtain allegedly infringing files by distributing bogus files. This practice is called interdiction. It is important to distinguish that this act is interdiction only in the definition of attempting to halt a specific activity (the user downloading an infringing file) and not in the definition of a court-ordained prohibition.

USER RISKS

The practice of interdiction can also be called pollution. It doesn't take place as a one-time only transaction in a vacuum. Interdiction has a cumulative effect on the both the individual user and the P2P networks that is detrimental and serious.

The user is taken advantage of and affected in many ways. The irony is that one would expect the entertainment industry to encourage the user to buy authorized content. But that is not what happens. No alternative is offered to the user. The entertainment industry punishes the user with a fake file but doesn't provide an authorized file. The only

practical option for the user is to try to download other illegitimate versions of the file or to migrate to other or more secure P2P networks that do not contain bogus files.

WHO'S THE HEAVY?

Interdiction in fact raises many more serious questions of legal liability on behalf of the copyright holder compared to the user.

- Entrapment. The downloading user is presumed guilty when that has not been determined or authorized by a court.
- Vigilantism. The copyright holder presumes it has the authority to act against the user.
- Fraud. The copyright holder clearly advertises the availability of a file with the listing of the file name and sharing of the file. But that is a false promise. The file is fake. This is worse than bait and switch as there is no indication of how to obtain an authorized file.
- Unauthorized appropriation of private resources. The use of bogus files does not just involve the downloading user. It involves the overall network and other users. When the copyright holder agent connects to the network, he takes up a connection slot to his direct connections that is denied to other users. When he is connected to the network he forwards search requests and results that may not reach other users because he's inserted himself into the network and other users are a connection further away from searching and sharing users. When he shares his bogus files, he causes his local network of users to use their computers and their Internet bandwidth on his behalf to perpetuate his entrapment and fraud. When the bogus files get propagated in the network (by users sharing the files with other users prior to actually checking the file) users throughout the network become co-opted and contribute their processing and bandwidth to abet the search and download of these files.

The significant number of bogus files results in a real impact on the overall network, including node availability, network horizon, and search speed and propagation to the detriment of all users. Lastly the copyright holder intentionally uses the private resources of other parties knowing that most users would not give their permission of said use if the copyright holder's intent were known.

- Bad corporate ethics. By using fraud and misappropriation of resources to share bogus files on the network, copyright holders sanction the activities of others who do the same, such as parties that distribute files that contain unwanted pornography, spyware, and viruses.
- Evasion of Corporate Responsibility. When a user obtains a bogus file he does not directly know what he has done wrong and who the guilty party is. The copyright holder does not provide their identification and justification in the bogus file.

- Restraint of Trade. Interdiction creates mistrust on the network. All content, authorized, legal, or not, is cloaked in its shroud of unreliability. All parties, including legal software developers and content providers are harmed. This clearly is the intent of copyright holders as no authorized files are provided on the P2P networks and there is no explanation or identification of copyright holders in bogus files. As a result the consumer assigns responsibility for the bogus files to the software developer or P2P network.

There is a clear example to support this. Prior to the summer of 2004 copyright holders concentrated interdiction on the Fast Track network used by Kazaa, Grokster, iMesh and other developers. Due to the interdiction Fast Track suffered greatly as its user base stopped increasing and started to decline. This effect was primarily due to interdiction as other P2P networks such as Edonkey continued to grow during this time. Interdiction, though aimed at the user, harmed Kazaa and other Fast Track developers. Equally importantly, interdiction harmed the Altnet paid download service hosted on Fast Track, the thousands of non-major label artists who used Altnet, and the many other content providers and distributors that were on Fast Track.

SUMMARY

Vigilante justice is never acceptable. RIAA's interdiction policy is more flagrantly unethical and illegal than Lycos's attack software distribution.

- There's a federal law against spam and courts have convicted spammers. In the US P2P file sharing software and networks are legal. There has been no court case yet decided of a consumer sued by RIAA.
- The spam software attacked a small group of people (tens of alleged spammers). Interdiction affects a much larger population (tens or hundreds of thousands of alleged infringers).
- Interdiction is directly performed by RIAA agents. Lycos's role was more indirect as independent individuals chose to download and run the Lycos software.
- Interdiction is founded on fraud and entrapment.
- Interdiction is not just a nuisance to the downloading user. It affects other users and the entire network, which are not a party to the alleged infringement.
- Interdiction causes real harm as in the Fast Track example.

In closing I submit one of those kindergarten rules that RIAA apparently forgot - two wrongs don't make a right.

Â

Marc Freedman

RazorPop, developer of [TrustyFiles](#), the leading multiple network P2P file sharing software

Read more articles at the [P2P Insider's Blog](#).

*Are you a major entertainment company or marketer? Then you need [BrandedP2P](#).
Are you an independent artist or small content provider? Check out the [Do-It-Yourself P2P Street Team](#).*