Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues

P2P File-Sharing Workshop – Comment, P034517

Comments of
The Recording Industry Association of America (RIAA)
November 15, 2004

P2P File-Sharing Workshop – Comment, P034517

Comments of
The Recording Industry Association of America (RIAA)
November 15, 2004

Table of Contents

I. USE OF P2P FILE-SHARING TECHNOLOGY 2

A. PERVASIVENESS OF PIRATED CONTENT 3
B. P2P ON CAMPUS 4
C. CENTRALIZED VS. DECENTRALIZED 6

II. IDENTIFICATION OF P2P FILE-SHARING SOFTWARE PROGRAM RISKS 7

A. PERSONAL INFORMATION 8
B. PORNOGRAPHY 9
C. SPYWARE AND ADWARE 12
D. DIMINISHED FUNCTIONALITY AND HIJACKED USAGE 14
E. VIRUSES 15
F. LITIGATION 16

III. LACK OF DISCLOSURE OF P2P FILE-SHARING SOFTWARE PROGRAM RISKS 19

IV. TECHNOLOGICAL SOLUTIONS TO PROTECT CONSUMERS FROM RISKS ASSOCIATED WITH P2P FILE-SHARING SOFTWARE PROGRAMS 22

V. THE ROLE OF P2P FILE-SHARING TECHNOLOGY IN THE ECONOMY 24

VI. P2P FILE-SHARING AND MUSIC DISTRIBUTION 27

VII. CONCLUSION 30

P2P File-Sharing Workshop – Comment, P034517

Comments of
The Recording Industry Association of America (RIAA)
November 15, 2004

The Recording Industry Association of America (RIAA), on behalf of its member companies, hereby submits these comments in response to the notice of the Federal Trade Commitssion (FTC) announcing a public workshop titled "Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues." The RIAA is a trade association whose member companies create, manufacture and distribute approximately 90 percent of all legitimate sound recordings sold in the United States.

The FTC's notice seeks comment on current uses of Peer-to-Peer (P2P) technology, and the effect of those uses on consumers and competition. P2P technology holds promise for many industries, including the recording industry. Unfortunately, as the recording industry forges ahead with new and diverse ways of providing music to consumers, record companies and artists have been undercut by the systematic and wholesale theft of their copyrighted works on certain P2P systems. The operators of these systems have deliberately structured their businesses to profit from this theft by attracting users to illegally copy music, movies, software, and other intellectual property. These P2P operators exploit this illegal activity without adequately protecting users from, or warning users of, the likely exposure to unwanted spyware, viruses, pornography, and the theft of sensitive personal information. The result of this activity includes millions of dollars and thousands of jobs lost to piracy, unfair competition for legitimate services attempting to bring music to consumers in new and exciting ways, and significant negative effects on individual consumers and the economy as a collective consequence of using these systems.

In addition, these P2P operators have intentionally architected their systems in an effort to offload liability for copyright infringement on individual consumers. They not only moved from a centralized to a distributed network in an attempt to secure immunity from liability, they also have regularly altered their system in order to thwart legitimate enforcement efforts of copyright owners. This course of conduct has had but one design– to perpetuate illegal "trading" of copyrighted works in order to protect ill-gotten profits.

Set forth below are comments addressing these and other issues included in the FTC's notice. The RIAA looks forward to exploring these issues at the public workshop and encourages the FTC to take appropriate action to protect consumers and to ensure fair and robust competition so that the potential of legitimate consumer applications of P2P technology can be achieved.

I. Use of P2P File-Sharing Technology

Since the arrival of the original Napster in 1999, numerous companies have jumped on the P2P bandwagon. While P2P is a promising technology that holds great commercial potential for content and other industries, many companies employing P2P technology to date have predicated their businesses almost entirely on the theft of copyrighted works. These companies receive substantial advertising revenue and licensing fees from third-party vendors who wish to reach a wide audience. Illicit P2P companies ensure this wide audience, and their own continued viability, by attracting users to their networks through the promise of stolen music, movies, software, and other intellectual property.

A. Pervasiveness of Pirated Content

Since the advent of the original Napster in 1999, P2P systems with unauthorized copyrighted content have exploded in size and popularity. In the month of October 2004, approximately 2.4 million users were on the FastTrack network (including Kazaa and Grokster) trading 1.4 *billion* files. In addition, 1.9 million users were on eDonkey at any given moment, trading 217 million files.[1] Considering these are just two of the networks currently available, the level of infringement encountered on illicit P2P services is staggering. By contrast, there were 48.6 million digital files sold through legitimate online services during the entire first half of 2004.[2]

It is difficult to overstate the rapid expansion of P2P usage in this country and the correspondingly large scope of the threat to America's creative community. In a 2003 study of the Gnutella network, Palisade Systems found that 97% of all activity on this system was illegal. Of the audio files alone, copyrighted works accounted for 99% of all requests made.[3]

The prevalence of pirated material online, and the organized structure of groups that prepare this content for illicit P2P networks, has been made clear by enforcement actions such as the Justice Department's "Operation Fastlink" in April of this year. In a sweep involving more than 10 countries (including the United States), more than 200 computers were seized, collectively containing hundreds of thousands of copies of pirated

[1] Source: MediaSentry.
[2] Source: 2004 RIAA Mid-year Statistics.
[3] Palisade Systems study, 3/3/03.

works, conservatively estimated at over $50 million. According to the press release, "Conservative projections of the losses to industry attributable to these distribution hubs are in the hundreds of millions of dollars."[4] These underground hubs, however, remain the tip of the iceberg, as much of the content they pirate ends up being traded to millions over illicit P2P services.

B. P2P On Campus

Young people are frequently early adopters of new technology, and several studies confirm that illegal file-sharing is extremely prevalent among teenagers and college students. According to Forrester Research, 49% of 12 to 22-year olds illegally downloaded in July 2003.[5] With regard to older youth, *Student Watch* from the National Association of College Stores reported that 54.6% of college students downloaded music without paying in 2002 (with an additional 14.9% "preferring not to say").[6]

As the costs of storage and bandwidth have decreased, and the speed of networks increased, the figures above likely have grown and will continue to grow. Nowhere is this more evident than on the college and university campuses across the country. Students who have grown up in a file-sharing culture dismissive of the importance of protecting copyrighted works, arrive at school to a utopia of extremely fast and convenient computer networks.

The Joint Committee of the Higher Education and Entertainment Communities, formed in December 2002 to work collaboratively to address the problem of unauthorized

[4] "Justice Department Announces International Internet Piracy Sweep," Department of Justice, 4/22/04.
[5] "From Discs to Downloads," Forrester Research, August 2003.
[6] eMarketer Spotlight Report, January 2004, citing *Student Watch* from the National Association of College Stores, August 2003.

file-sharing, reported on this issue to the Judiciary Subcommittee on Courts, the Internet, and Intellectual Property in October of this year. The report particularly noted that the increased speed of networks has created new challenges for copyright owners. For example, Internet 2 is a platform for advanced network applications and technologies run by a consortium of schools, industry, and government. Yet, as with other networks, bad actors have begun to hijack it, threatening to turn a beneficial and promising technology into a tool for piracy. Already, P2P systems, such as i2hub, have been set up on Internet 2, facilitating the abuse of advanced networking technology to illegally distribute copyrighted works for free. The speed of these networks—up to thousands of times faster than ordinary Internet networks—allows users to obtain copyrighted movies in *minutes* and music in *seconds*. Further, the closed nature of these networks, being available only to those engaged in academia, makes it more difficult for copyright owners to protect their works and to notify responsible parties of their infringement.[7]

[7] The naturally high speeds of college and university networks has also allowed students to set up local area networks—or LANs—to connect with others solely within their individual schools and behind the protection of the schools' firewalls. The RIAA brought suit last year against the student operators of four such networks, who had effectively used their school's resources to create "mini-P2P networks" to facilitate the mass piracy of copyrighted works on their campuses. As with Internet 2, the closed nature of these LANs makes it difficult to discover such illegal activity.

C. Centralized vs. Decentralized

The original Napster[8] was based on a central server system. After downloading the Napster P2P software, a user logged into the company's main server, which then catalogued all the files available in that user's "share" folder on his computer. Napster maintained this database of users' available files, and allowed users to search each other's catalogue. The system then essentially became an online swap meet, where Napster facilitated the trading of files. A person who typed in the name of a particular file was informed of other online users who possessed that file. With a simple click of the mouse, that person could then download the desired file from another user.

Because it maintained a central server database and facilitated the illegal trading of copyrighted music, the original Napster was found liable for copyright infringement.[9] This ruling by the Ninth Circuit Court of Appeals led those interested in facilitating and inducing the continued illegal trading of copyrighted materials to develop and exploit new forms of P2P. The result was the sprouting of decentralized P2P networks that relied on a distributed architecture to avoid a centralized function that was seen as the linchpin of the Ninth Circuit's ruling.

Decentralized P2P networks rely on each user ("peer") to facilitate the browsing and downloading of files. Both searches and transfers (as opposed to just transfers in the centralized system) are made *directly* between users, with no critical need for a central host such as the Napster server.

[8] RIAA's member companies filed suit against the original Napster in December 1999. Following several major rulings in favor of the record companies, the original Napster ultimately went bankrupt. The current version of "Napster" that operates today is a legitimate service utilizing the original Napster name and logo, but in all other relevant aspect is structured completely differently than the original Napster discussed herein.

[9] *A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).*

Importantly, to most users there is no apparent difference between the central and decentralized P2P systems while trading files. The functionality behind these networks is generally transparent—all one needs to do is type in a search term and click on a suggested link. The steps are presented to users in the same manner regardless of the methodology.

However, while there appear to be benefits to users of a centralized P2P system, such as enhanced security and reliability, providers of illicit P2P services have nonetheless consistently chosen to employ the decentralized model in an attempt to avoid legal liability. By doing away with the central server and offloading the peer-matching responsibility to end users, illicit P2P services have attempted to bypass the holding in the Ninth Circuit case and pass on their legal liability to millions of consumers.

Simultaneously, they have passed on a host of risks and dangers, such as viruses, spyware, exposure to adult and child pornography, and the unknowing disclosure of sensitive personal material. (These are discussed in more detail in the next section.) These illicit P2P services continue to tarnish a promising technology and remain a major threat to the future of creative works and the economy to which they contribute.

II. Identification of P2P File-Sharing Software Program Risks

Providers of many peer-to-peer (P2P) file-sharing software use deceptive and unfair practices to promote their products and mislead their customers about the level of privacy, security, and legal liability they may encounter when utilizing P2P services. With the proliferation of these applications, there is an increased threat of harm to tens of millions of computer users throughout the country. Although illicit P2P software providers promote and distribute their file-sharing products as “free,” there is, in fact, a high and undisclosed price to consumers, as detailed below.

While illegal file-sharing has had a severely damaging and much-publicized effect on the music and other entertainment industries, computer users, as well as entire companies and businesses, are increasingly harmed by the actions of illicit P2P networks. The unaccountability of the providers of these applications ensures the continued proliferation of dangers such as viruses, spyware, and the unknowing disclosure of sensitive personal material.

A. Personal Information

P2P services, by their very nature, are dependent upon users not only downloading, but providing material on their computers for others to access. To facilitate this two-way sharing, P2P services often configure their software to share content by default. What users often do not know is that they may be sharing their tax returns, financial records, health records, business records, email, and other personal and private material. The availability of such information threatens security and facilitates identity theft.

As an initial matter, P2P software may, upon installation, automatically search a user’s *entire* hard drive for content. Files that users have no intention of sharing may end up being offered to the entire P2P network.[10] Continued sharing of personal information is hard to avoid and is facilitated by confusing and complicated instructions for

[10] “Music Downloading, File-Sharing and Copyright,” Pew Internet & American Life Project, July 2003; *see* “File-sharing: A Fair Share? Maybe Not,” FTC Consumer Alert, July 2003. (“If you don’t check the proper settings when you install the software, you could open access not just to the files you intend to share, but all other information on your hard drive.”)

designating shared items.[11] A study by Nathaniel S. Good and Aaron Krekelberg at HP Laboratories showed that "the majority of the users…were unable to tell what files they were sharing, and sometimes incorrectly assumed they were not sharing any files when in fact they were sharing all files on their hard drive."[12] Distributors of file-sharing software are clearly aware of the likelihood of such inadvertent sharing. Greg Bildson, COO of LimeWire, said that "more can be done to warn users when they are about to share large numbers of files…. For users that don't know what they are doing, file-sharing applications need to be a little more bulletproof."[13]

As one news site has pointed out, available information goes beyond the relatively benign home shopping list or personal résumé. "Military members take their personal computers into a theater of operations and then return from those areas without removing sensitive information from their hard drives."[14] This unintended sharing affects not only individual consumers, but also potentially our national security.

B. Pornography

In addition to the dissemination of personal information, users also run the risk of being inadvertently exposed to pornography on these systems. In an August 5, 2004 letter to file-sharing association P2P United, 47 U.S. Attorneys General noted that a "substantial and ever-growing use of P2P software is as a method of disseminating pornography, including child pornography."[15] In fact, a 2003 study by Palisade Systems

[11] *See* Letter to FTC from Senators Leahy, Hatch, Boxer, Stevens, and Smith, 5/4/04 ("Senator Letter 5/4/04").

[12] "Usability and privacy: a study of Kazaa P2P file-sharing," Good and Krekelberg, 6/5/02.

[13] "What's in Your Shared Folder?" Slyck.com, 7/30/04.

[14] *Id*. (quoting commentator from www.SeeWhatYouShare.com)

[15] Letter to P2P United from 47 U.S. Attorneys General, 8/5/04 ("AG Letter 8/5/04").

found that 42% of all requests on a file-sharing network were for adult or child pornography (a full 6% being for child pornography).[16] The prevalence of such content, and the alarming accessibility by young computer users, is made apparent by a simple search for pop stars or children's shows, which invariably brings up results laden with pornographic material.

The seriousness of this issue has been widely recognized and brought to light. In February 2003, the General Accounting Office issued a report entitled "Peer-to-Peer Networks Provide Ready Access to Child Pornography."[17] According to the report, a search of twelve keywords known to be associated with child pornography on the Internet resulted in a list of files comprised of 42% child pornography. Searches for more innocuous keywords (such as cartoon characters and celebrities) returned images including adult pornography (34%), cartoon pornography (14%), child erotica (7%), and child pornography (1%). These files are freely available at the click of a mouse, accessible to all, including unsuspecting children.

Further, the automatic sharing feature of P2P software threatens users with violation of criminal law. A May 4, 2004, letter from five U.S. Senators to the FTC noted that some illegal child pornography "is mislabeled so it will appear in response to innocuous searches."[18] This may enable a user to unknowingly "redistribute violent pornography to children and others – and risk criminal prosecution under state or federal

[16] Palisade Systems study, 3/3/03.

[17] "File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography," General Accounting Office Report to the Chairman and Ranking Minority Member, Committee on Government Reform, House of Representatives, February 2003.

[18] Senator Letter 5/4/04, *supra* note 11; *see also* "File-sharing: A Fair Share? Maybe Not," *supra* note 10. ("You may unwittingly download pornography labeled as something else.")

criminal laws governing pornography distribution."[19] P2P services have not made known the threat of these mislabeled files or, as discussed above, the potential legal (and criminal) liability of users.

Finally, parents have a legitimate interest in considering the types of entertainment to which their children are exposed. The FTC has noted that associations such as the RIAA continue to take positive and successful steps toward empowering parents in this regard, such as providing appropriate notices and labeling in advertising and packaging of music. Simultaneously, providers of P2P software work to erode that level of control and informed consent by allowing anyone access to unlabeled music, images, and video files of virtually any kind. In addition, the mislabeling of files provides access to inappropriate works even without users' intent. (A search by a teenager for a Britney Spears video will often bring up porn.) P2P services not only fail to provide for the type of labeling now universally adopted by legitimate distributors; they make no significant effort of any kind to notify parents of the types of materials their children will find when they start "sharing" files with anonymous fellow P2P subscribers of all ages and tastes.[20]

While some P2P applications offer the capability to filter pornographic content, the option is frequently rendered useless by ineffective methodology, including limited keyword filters that often miss offensive (or illegal) files hidden behind innocent names.[21] Further, the ability to circumvent such filters is laughably simple. In at least

[19] Senator Letter 5/4/04, *supra* note 11, at 3. *See also* "Cyber Education Letter," FBI (http://www.fbi.gov/cyberinvest/cyberedletter.htm); "Peer-to-Peer Software Providers' Liability Under Section 5 of the FTC Act," FTC filing by Howrey Simon Arnold & White, LLP and The CapAnalysis Group, LLC, April 27, 2004, at 22 ("Section 5 Liability paper").

[20] *See* Section 5 Liability paper, *supra*.

[21] *See* Senator Letter 5/4/04, *supra* note 11.

one case, after a search returned pornographic material, a pop-up window appeared asking if the user would like to "disable the adult filter." This was accompanied by an option to automatically do so in the future without even seeing the pop-up window. Such options render useless parents' attempts to protect their children.

C. Spyware and Adware

P2P applications are also often bundled with third party spyware (or P2P services' preferred euphemism "adware"),[22] hijacking a user's computer without his or her knowledge. Such third party software is used to produce targeted advertising by gathering detailed information stored on a user's computer, including personal identification and web-browsing activity, which is then automatically relayed to a web server typically without the user's knowledge. While the purpose and result of such activity is seemingly transparent, the dangers of spyware and adware are manifold:[23]

- Compromises privacy by transmitting information about a user's behavior;
- Decreases usability and productivity due to the appropriation of a computer's or network's broadband capacity (resulting from the constant transmission of personal information and receipt of targeted advertisements);
- Hijacks a user's computer storage space and network when third parties secretly commandeer (and even sell) these valuable resources;

[22] Spyware may also be acquired through the network's shared files. *See* Center for Democracy & Technology, Comments and Request to Participate: FTC April 2004 Spyware Workshop at 2 (March 5, 2004) ("'Spyware'…maybe bundled with other free applications, including peer-to-peer file-sharing applications [or] maybe be distributed through deceptive downloading practices.")

[23] *See* Section 5 Liability paper, *supra* note 19, at 9-18; "File-sharing: A Fair Share? Maybe Not," *supra* note 10; TruSecure Press Release 12/29/03 ("TruSecure"), noting the "emergence of problems associated with 'Spyware' piggybacking programs that come with free software."

- Increases spam email after the furtive acquisition of a user's email addresses and phone numbers; and
- Augments impact of such applications, causing permanent and continued activity due to the difficulty of deletion, automatic updates, and evasion of anti-spyware tools.

In addition, "registration data is regularly sold to direct marketing firms."[24]

While many P2P software providers claim to be adware- and spyware-free (with bold statements such as Limewire's "[n]o spyware…EVER!"), such claims are likely deceptive. Other P2P providers use misleading descriptions of the spyware affiliated with their service. For example, eDonkey describes its bundled software as "promotional software" which "can add new functionality"; Morpheus describes it as "value added software." This euphemistic language serves to convince users of the desirability of such applications, but fails to acknowledge the hidden costs outlined above.

In addition, many statements regarding third-party software are often outright false. Morpheus claims "no spyware" if a user upgrades to a pay service. Yet, further investigation shows that spyware from the basic version remains active following a user's upgrade. Morpheus also claims "no bundled software" in its upgrade, but the option to include spyware is selected as a default when accepting the relevant terms and conditions; users who do not <u>un</u>check the appropriate box will nevertheless receive unwanted software.

Disclosure regarding the inclusion and functionality of third party software, if made, is often buried in the fine print of the End User License Agreement (EULA). Such

[24] "P2P Fear and Loathing: Operational Hazards of File Trading Networks," John Hale, Nicholas Davis, James Arrowood, Gavin Manes, September 2002, at 2.

inadequate disclosure usually further refers users to the license agreements of (undisclosed) purveyors of the bundled third party software, disclaiming any responsibility for the inclusion and effect of such hidden applications. Notably, many P2P programs cannot be acquired without such spyware, and are often rendered inoperable when such spyware is removed.[25]

D. Diminished Functionality and Hijacked Usage

The presence of bundled third-party software highlights another risk to users of illicit P2P networks. This software, and, indeed, the P2P applications themselves, often run in the background without the user's knowledge. The July 2003 FTC Consumer Alert noted that "closing the file-sharing program window does not actually close your connection to the network," and that "some file-sharing programs automatically open every time you turn on your computer."[26]

In addition, the nature of decentralized P2P networks requires certain computers to act as "supernodes" (or "ultrapeers"). These computers, which replace the hub in a central server P2P model, belong to users throughout the file-sharing networks, and are almost always designated without the users' knowledge. Such designation essentially makes these end users a type of client index, where other users come in order to search for shared files. EULAs generally fail to mention this practice and any discussion on the topic is often highly technical or couched in confusing or deliberately benign language.

[25] Palisade Systems, Executive Summary of Peer-to-Peer Study Results at 2 (March 2003) ("Applications such as KaZaA and BearShare require users to install spyware on their computer as part of the licensing agreement.")

[26] "File-sharing: A Fair Share? Maybe Not," *supra* note 10; *see* AG Letter 8/5/04, *supra* note 15.

These hidden or inadequately stated practices can affect the functionality of users' computers by reducing available bandwidth, processor capacity, memory, disk space, and security. Such practices harm users by consuming services that could be otherwise used for legitimate purposes.

Unauthorized P2P applications have also had a significant impact in the academic environment, affecting institutions of higher education, including public universities. In May 2004, the General Accounting Office reported that higher education institutions had spent additional funding during the 2003 to 2004 academic year for "a variety of network infrastructure and operational areas, including bandwidth expansion, bandwidth management, software/hardware, system management, and system maintenance."[27] The additional funding was made necessary in large part due to the presence of P2P applications on their networks.

E. Viruses

The July 2003 FTC Consumer Alert also noted that downloaded files could contain "a virus or other unwanted content."[28] According to a study done by TruSecure, "45% of the free files collected via KaZaA…were viruses, Trojan horse programs and backdoors."[29] This malicious code can have devastating consequences for users, up to and including destroying all the content on a computer. A report by researchers at the University of Tulsa noted that, whether or not a virus itself affects a user's computer, "the massive reproduction of self-replicating code may be enough to cripple hosts or regions

[27] "File-sharing: Selected Universities Report Taking Action to Reduce Copyright Infringement," General Accounting Office, May 2004, at 10.

[28] *See* "File-sharing: A Fair Share? Maybe Not," *supra* note 10.

[29] *See* TruSecure, *supra* note 23.

of a network."[30] The "open community" of P2P networks makes them ideal for passing on this malicious code. As the FBI warned, "some worms have been specifically written to spread by popular Peer-to-Peer networks."[31]

Illicit P2P applications have been woefully inadequate in conveying the risks to consumers of viruses, worms, Trojan horses, and other forms of malware. The claims by some services that their application includes anti-virus software offers false security against a constantly mutating threat and fails to inform users of the dangers inherent in a system based on connecting anonymously with others.

F. Litigation

The lack of recourse against decentralized P2P services to date has forced copyright owners to sue users of P2P systems who are illegally downloading. Since September 2003, the RIAA has filed over 6,000 lawsuits against users of P2P services who have illegally traded music files. The MPAA recently announced it will similarly begin filing lawsuits against those illegally distributing copyrighted movies.

While P2P services certainly are aware of the use of their software to illegally exchange copyrighted works, there is often insufficient notice to users. The New York Times reported on a sense of confusion to some created by the mixed messages from P2P services on what is right and wrong. One student in a discussion among 7th and 8th graders asked, "Why isn't there a warning that what we're doing is illegal?"[32]

[30] "P2P Fear and Loathing: Operational Hazards of File Trading Networks," *supra* note 24, at 3.

[31] *See* "Cyber Education Letter," *supra* note 19.

[32] Letter to P2P Executives from Senators Graham, Feinstein, Durbin, Smith, Cornyn, and Boxer, 11/12/03 ("Senator Letter 11/12/03"), citing "Is It Wrong to Share Your Music? (Discuss)," Katie Hafner, The New York Times, 9/18/03.

While there are services that claim to inform users of the legal considerations of their file-sharing, these notices often remain inaccessible, deliberately vague, or outright misleading. Frequently, any such notice is buried in the software's EULA at installation. These agreements, highly technical and lengthy, are usually overlooked by users. Even if users manage to wade through the fine print, any warnings are tempered by further statements and claims of the services. For example, Morpheus claims to be the "only legally sanctioned peer-to-peer file-sharing application based in the U.S." Such a statement, a twisted interpretation of the *Grokster*[33] decision of the Ninth Circuit, is intended to give users the impression that *any* use of this "legally sanctioned" application is inherently legal. Morpheus further misleads consumers by stating that "users can receive FREE Downloads of non infringing material." Such unqualified statements fail to clarify the fact that much (indeed, most) material users may download is infringing.

Other services also participate in misleading users about the legality of their potential conduct. In Lime Wire's Frequently Asked Questions, for instance, a question as to whether the service is legal is answered simply by stating, "Yes, it is legal to use Lime Wire's software. It is an Internet enabling technology."[34] There is no mention of violating federal law by illegally trading copyrighted works. Similarly, eDonkey prompts its users to "Download popular files…." While the most popular files on P2P networks are commercial songs and movies, there is no concurrent discussion about copyright protection or theory.

Further illustrating their awareness of such legal risks and their refusal to guide users appropriately, some providers have begun to develop new software versions

[33] *MGM Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. Cal. 2004).*

[34] LimeWire Frequently Asked Questions (http://www.limewire.com/english/content/downloads/presskit/faq.pdf).

supposedly designed to circumvent detection of users' identity. For example, BearShare claims "complete anonymity for users" and LimeWire claims "Users can now…protect their identity." Such claims of anonymity lead unsuspecting consumers to mistakenly believe they are safe from being sued.

By using misleading statements and failing to include warnings, illicit P2P services truly do a disservice to their users since infringers of copyright law are subject to strict liability. It is no defense for a user to claim he did not know his activity was illegal. While awareness has grown that trading copyrighted works on these illicit networks is a violation of federal law, the inappropriate claims and omissions by these companies presents a situation where users may mistakenly believe they can get away with what they know to be illegal. Infringement of copyrighted works carries severe penalties, including up to $150,000 *per infringed work* (each file traded on P2P). Criminal liability can even carry prison terms. These are real and significant risks, and P2P providers do their users an immense disservice and great harm by failing to acknowledge them.

III. Lack of Disclosure of P2P File-Sharing Software Program Risks

Many P2P networks remain rife with the threat of exposure to pornography, spyware and adware, diminished functionality, viruses, and litigation, as well as the potential to share personal information. Despite this, several authorities have documented the failures of illicit P2P services to warn users about the risks and dangers present on file-sharing networks, and to configure their software to provide a safe and legitimate product. In their "Usability and privacy" study mentioned above, Nathaniel Good and Aaron Krekelberg suggested that P2P applications "do a poor job of preventing users from sharing potentially personal files," and that changes should be made to ensure users' security.[35]

The May 4, 2004, letter from five U.S. Senators to the FTC noted the responsibility of P2P services to "effectively educate even their youngest users about the dangers of their software," and requested the Commission to investigate these issues and the services' performance of their obligations.[36]

The services have also been informed directly about the need for them to guard and warn against such dangers. The November 12, 2003, letter to several P2P service executives, signed by six U.S. Senators, urged these businesses to voluntarily take three steps toward becoming legitimate and responsible participants in the online community: (1) Provide a clean, conspicuous, and meaningful notice and warning to users about the legal risks of using P2P software, (2) incorporate effective copyright and pornography filters, and (3) change the "sharing" default setting.[37]

[35] *See* "Usability and privacy: a study of Kazaa P2P file-sharing," *supra* note 12.
[36] Senator Letter 5/4/04, *supra* note 11.
[37] Senator letter 11/12/03, *supra* note 32.

Unfortunately, even despite the August 5, 2004, letter to P2P United signed by 47 U.S. Attorneys General encouraging its member companies to "take concrete and meaningful steps to address the serious risks posed to [] consumers" by P2P technology,[38] these illicit P2P services have taken no action to address these issues.

These companies' lack of interest in legitimacy is further evident in their refusal to accept other methods of education and enforcement. For example, since a large proportion of traffic on P2P sites is for copyrighted music and movies, it would seem reasonable for these applications to link or refer to information sites, such as www.MusicUnited.org, or to legitimate services for those interested in obtaining legitimate product (such as iTunes, RealNetworks, Napster, and Cdigix). Offering information only from one-sided sources that promote the acceptance of unauthorized file-sharing harms users by misstating the issues and understating the risks and dangers. As an example, in a frequently asked question on piracy, Lime Wire merely states its belief that current laws are over-reaching and makes no effort to inform users either of the potential to infringe using its network or of their obligations under the law.[39]

In addition, some P2P services have taken actions to specifically thwart the efforts of copyright holders and law enforcement officials to protect copyrighted works. When copyright holders began using the Instant Messaging feature included in some P2P software to inform users that they may be engaging in infringing activity, the P2P service immediately deactivated it. Some services also deactivated their shared library browsing

[38] AG Letter 8/5/04, *supra* note 15.

[39] From LimeWire's Frequently Asked Questions: "What is LimeWire's position on piracy? LimeWire is working to keep P2P technology legal in the courts and in Congress. The company defends Freedom of Speech and believes that existing laws are an over-reaching abuse of copyright laws. The company believes that there is no way to control piracy in a file sharing system…" (http://www.limewire.com/english/content/downloads/presskit/faq.pdf).

feature, which allowed users to find more files from the same user, after discovering that it provided a means for copyright holders to enforce their rights. Other services have interfered with the "spoofing" efforts of copyright holders. Further, some services no longer require unique usernames and even offer default "anonymous" usernames. As a more startling example of an effort to thwart enforcement, BearShare's EULA outrightly prohibits certain copyright enforcement vendors and associations from installing and using its software. Such actions are in no way beneficial to responsible P2P users and serve no purpose other than to frustrate and block the efforts of content owners to protect their rights (thereby ensuring the continuation of the mass infringement on these networks).

Finally, some services have begun to use encryption. This feature defeats the ability of network administrators to manage their network usage and prevent abuse of computing resources. In addition, as the Attorneys General noted in their letter to P2P United, services' addition of "encryption features will make it more difficult, if not impossible, for law enforcement to police users of P2P technology in order to prosecute crimes such as child pornography. Encryption only reinforces the perception that P2P technology is being used primarily for illegal ends."[40]

There are concrete steps here for illicit P2P services to take in order to become responsible participants in the online community. To date, however, these services have shown no interest in embracing this path to legitimacy. Indeed, they have taken affirmative steps in the opposite direction, seeking to reinforce their ability to promote illegitimate uses.

[40] AG Letter 8/5/04, *supra* note 15.

IV. Technological Solutions to Protect Consumers from Risks Associated with P2P File-Sharing Software Programs

The November 12, 2003, letter from six U.S. Senators to executives of several P2P services included in its list of steps toward legitimacy a call to "incorporate effective copyright and pornography filters."[41] The letter stated the following:

> Two well-respected technologists recently pointed out that your company could easily take steps to reconfigure your software to significantly reduce or prevent copyright infringement and pornography. According to Professor Leonard Kleinrock of the UCLA Computer Science Department: "There is nothing inherent in the technology…of peer-to-peer system[s] that would prevent [them] from taking steps to prevent or greatly diminish the volume of copyright infringement on their systems." And Darrell Smith, the former CTO of the file-sharing service Morpheus (StreamCast Networks) noted that: "Peer-to-peer file sharing applications already filter those things that their users do not want, such as bogus music files and viruses. They could very easily adopt and implement a filter to eliminate unauthorized copyrighted works as well, but user levels and revenues could decline if popular music or movie files were filtered."[42]

While Mr. Smith has recognized the true reason that illicit P2P services eschew implementing effective filters and other technological measures—namely a desire to reap the rewards of a system based on infringement—other responsible entities have begun to use these new hardware and software technologies to great success. This has been particularly notable on the campuses of higher education.

In two reports to the Judiciary Subcommittee on Courts, the Internet, and Intellectual Property, the Joint Committee of the Higher Education and Entertainment Communities reported that several schools have implemented technological measures to

[41] Senator Letter 11/12/03, *supra* note 32.
[42] *Id*. at 2.

combat illegal activity on their networks.[43] Three of these technologies were specifically highlighted: ICARUS, ACNS ("Quarantine"), and CopySense.

ICARUS, an application designed to automatically prevent infringement through P2P services on the University of Florida network, processed 6,503 Acceptable Use Policy violations, including P2P violations, during its first three months of use (starting in June 2003). In that period, the system had only five false positives out of 6,508 detected violations, and none of them were related to P2P activity. The school is now planning to license the system to other schools.

"Quarantine," implemented at UCLA and based on Sony's ACNS technology, is an automated system that streamlines the notification of, and penalty for, copyright infringement. After receiving notice that a user is illegally sharing files, the Quarantine system automatically shuts that user out of the school network. To restore access, the user must visit a web site where he agrees to abide by the school's acceptable use policies and to remove the infringing material from his computer.

Audible Magic's CopySense system, which uses filtering technology to weed out infringing transmissions, has also been installed to great effect on several school networks, including Concordia University, Coppin State University, Texas A&M, and Wittenberg University. CopySense generates digital fingerprints for audio content by electronically "listening" to the song or audio file, enabling authorized files to still be

[43] "Progress during the Past Academic Year Addressing Illegal File Sharing on College Campuses," Joint Committee of the Higher Education and Entertainment Communities report to the Subcommittee on Courts, the Internet, and Intellectual Property, House Judiciary Committee, August, 2004; "Peer-to-Peer (P2P) Piracy on University Campuses: An Update," Joint Committee of the Higher Education and Entertainment Communities report to the Subcommittee on Courts, the Internet, and Intellectual Property, House Judiciary Committee, October 2004.

traded, but blocking transfers of copyrighted files.[44] With CopySense installed, IT administrators have reported reclaiming half of their network's bandwidth at significantly reduced costs. One school went from weekly notices of infringement to none at all.

These products have shown that filtering is indeed an effective means of curbing illegal activity on P2P networks.

V. The Role of P2P File-Sharing Technology in the Economy

Again, while P2P technology may ultimately offer the promise of increased efficiency and productivity, applications such as Kazaa and Grokster are used almost exclusively for illegally trading copyrighted works. The adverse effect on the economy from these services is manifest. In addition to increasing bandwidth costs for activity unrelated to the business or purpose of the network provider, illicit P2P services pay no taxes on the bulk of their "products"; decimate a vital creative industry; facilitate illegal activity; expose users to viruses and spyware; expose users' personal information (including tax returns, medical records, and resumes); rob artists, songwriters, and copyright owners or their rightful royalties; and expose users to pornography. In contrast, legitimate services pay millions of dollars in taxes, create tens of thousands of jobs, contribute to a positive trade balance, compensate creators, respect the law, protect consumers' private personal information, and include parental controls.

Illicit P2P services are, in fact, largely a liability for businesses, especially considering the inherent risks posed by viruses and spyware often accompanying the software. This fact has been widely recognized in the government workplace, as several

[44] "Audible Magic's CopySense Appliance," http://www.audiblemagic.com/news&press/press_20031021.html.

federal and state organizations have issued orders severely limiting or prohibiting outright the use of unauthorized P2P systems. The U.S. Departments of Justice, Commerce, and Agriculture, for example, have warned employees not to use or install these applications on their computers, finding among other things that "These 'evasive' programs…have no recognized business need."[45] The Office of Management and Budget has also issued a Memorandum on "Personal Use Policies and 'File Sharing' Technology" to ensure that "the proper controls are in place to prevent and detect improper file sharing."[46] In addition, Governor Schwarzenegger in California issued an Executive Order on September 16, 2004, recognizing that "…the presence of certain peer-to-peer file-sharing software on state computers presents a significant security risk…may permit viruses and other malicious programs…consumes network resources…and enable[s] illegal dissemination and downloading of copyrighted material, including music, motion pictures, software and video games, resulting in huge losses of revenue to the state's valuable entertainment industry."[47]

In some situations and for some applications, P2P architectures may help optimize network resources, including storage, processing and bandwidth. But P2P networks also pose significant challenges with respect to resource management, security and authentication. In general, the comparative efficiency of P2P versus client-server systems depends upon a complex set of technological and market factors relating to the relative costs and capabilities of network resources (e.g., bandwidth; central vs. distributed storage).

[45] "Interim Guidance on Peer-to-Peer Software and Copyright," U.S. Department of Agriculture (http://www.usda.gov/da/IRD/CS-010.htm).
[46] "Personal Use Policies and 'File Sharing' Technology," Office of Management and Budget (http://www.whitehouse.gov/omb/memoranda/fy04/m04-26.html), 9/8/04.
[47] California Executive Order S-16-04 (9/16/04).

The economically optimal use of P2P infrastructures will be achieved only when property rights are well defined and respected, market participants are well informed and market mechanisms are able to operate. With respect to the consumer-oriented P2P systems that are the focus of the FTC's workshop, none of these criteria are met. The current system depends not only on theft of intellectual property, but also on market and information failures that prevent P2P participants from shouldering the full costs of their activities in terms of bandwidth usage, distribution of viruses and "malware," utilization of computer memory and processing resources, etc.

There is no evidence of which we are aware that the current generation of commercial P2P networks is economically efficient, even in the limited sense of optimizing computer and communications resources. The major obstacle to efficiency is a business model based on theft. Again, P2P technology holds the promise for many legitimate uses, including music distribution. But legitimate businesses obviously find it difficult to compete with illegal uses of P2P.

Despite the obstacle of illicit services, one notable attempt to harness the power of P2P for legitimate goals is Penn State University's LionShare project (slated for release in 2005). Now a collaborative effort between Penn State, MIT, Open Knowledge Initiative, researchers at Simon Fraser University, and the Internet2 P2P Working Group, LionShare is an effort to provide legitimate file-sharing capabilities for individuals and educational institutions. Specifically, LionShare "builds on average peer-to-peer technology to include all the personal file-sharing capabilities of Kazaa and Gnutella, plus adds the novel features of authentication, access control, copyright protection, and permanent ‘continually on’ storage space.”[48] The considerable interest in the LionShare program from around the world is evidence not only of the potential for legitimate P2P applications, but also of the significant concern of responsible organizations for the continued harm from the use of illicit file-sharing services.

VI. P2P File-Sharing and Music Distribution

The music industry is currently in a multi-year period of decline. According to the most recent year-end figures, the total value of units shipped fell 18% from 1999 to 2003.[49] The industry’s top 50 albums shipped 16.7% less in the first half of 2004 compared to three years ago, and the top 100 albums shipped 19.7% less. Progressively declining sales of the top albums are devastating to the music industry because the financial return on these “top” artists largely covers record company losses for the majority of remaining acts in which record companies invest substantial sums that are never recouped. These artists, in essence, support the industry and fund the ongoing efforts to discover and nurture new talent. The illegal file-sharing activity on illicit networks is quickly destroying the industry’s ability to bring this talent to the world and is robbing the public of a more prolific and creative future.

Throughout the attack by illicit P2P services, the music industry has endeavored to bring users content in new ways, including through legitimate music download services such as iTunes, MusicMatch, and (the now legitimate) Napster. For the first half of 2004, there were 58 million single tracks downloaded or burned from licensed online

[48] http://lionshare.its.psu.edu/main/

[49] Based on total suggested retail list prices of shipments. Source: RIAA.

music services.[50] That figure is dwarfed, however, by the estimated 7.1 *billion* downloads that will be made illegally in 2004.[51] Though certainly gaining ground, the continued progress of legitimate services is directly impeded by the unauthorized offering of identical product for free by illicit P2P services.

As Michael Weiss, Chief of Streamcast Networks (distributor of Morpheus) has said, "Users are likely to abandon any file-sharing network that restricts their downloading in favor of the many networks that don't."[52] (Also note the statement of Wayne Rosso, former President of Grokster that, "…the problem is that even though the opportunities are starting to arise now and the record companies are reaching out, many of my colleagues are backing off, afraid that if they play ball they'll lose their traffic.")[53]

An August 2003 report from Forrester Research concluded that "To succeed with on-demand media services, entertainment companies will need to: 1) slow online piracy through technical and legal action, and 2) support the creation of on-demand alternatives."[54] Attempts to address the first part are ongoing, with educational initiatives such as creative content industry letters to schools, businesses, and major news outlets, and by independent websites such as www.MusicUnited.org. The MPAA also initiated a public service announcement before feature films in theaters about the harm from illegal file-sharing. Supplemental efforts have included the series of lawsuits brought by the music industry (and, later this month, by the movie industry), and by digital rights management and other forms of protecting content. In addition, as the Joint Committee

[50] Source: RIAA
[51] "The State of the Industries: Past, Present, and Future," McKinsey & Company, Inc., 11/4-5/03.
[52] "Sony BMG, Grokster Join Forces," Los Angeles Times, 10/29/04.
[53] "RIAA Finally Considers P2P," digital music news weblog, http://www.digitalmusicnews.com/blog/116, 11/15/04.
[54] "From Discs to Downloads," Forrester Research, August 2003, at 8.

on the Higher Education and Entertainment Communities reported to Congress on October 5, 2004, we continue to reach out to colleges and universities across the country as they engage students in discussions on P2P and copyright, and as they seek new legitimate ways to bring content to their campuses.

The second suggestion by Forrester continues to be addressed as well. To date, there are no fewer than 50 sites on the web where consumers can get quality legitimate product. The Joint Committee of the Higher Education and Entertainment Communities has noted great strides in this area on university and college campuses. According to a report in August of this year, at least 20 different schools had signed up to provide a means for students to get a wide range of entertainment content legally and easily. That number, since raised to 33, continues to increase as positive reception of these services is reported.

Whether on campuses or in private homes across the country, these legitimate download services (such as iTunes, Cdigix, RealNetworks, Napster, Ruckus, and MusicRebellion) offer consumers a host of benefits. In contrast to the black market bazaar of illicit P2P networks, legitimate download services offer clearly legal product free of viruses, spyware, adware, and corrupt content, as well as good connections and no "free-riding" on users' bandwidth or processing power. In addition, notices and labeling remains intact, allowing consumers and parents to make informed decisions about whether content is appropriate for them. And, of course, legitimate services provide an infrastructure to ensure that creators, producers, providers, and the thousands of individuals who work hard to bring consumers the products they enjoy, are appropriately compensated for their hard work.

The recent and notably rapid flourish of legitimate online distribution services has been made possible by the aggressive licensing of record companies, movie studios, artists, and other copyright holders. The world of copyrights and ownership is an extremely complex web, but the content industry recognizes the promise of digital delivery and has worked hard to provide consumers with the product they desire in the format they want. The Forrester report itself "didn't find a single executive stuck on the idea of 'defending the status quo' of selling physical objects."[55] The content community remains willing to work with any provider of technology or service, including P2P, which recognizes, respects, and enforces the rights of copyright holders and the value of their works.

VII. Conclusion

We encourage the FTC to address the problems for consumers and the economy that are posed by those who have hijacked P2P technology for short-term gain. We look forward to working with the FTC and all interested parties to ensure a robust, safe, and legitimate future for P2P.

[55] *Id.*