P2P Frequently Asked Questions (FAQ)

P2P Frequently Asked Questions (FAQ)

Below is a list of some frequently asked questions about peer-to-peer (P2P) file sharing and software. P2P software and copyright infringement are often linked together. This page covers primarily questions in regards to the P2P software and how it shares files.

To learn more about copyright issues at MIT go to: Copyright at MIT or visit Copyright Frequently Asked Questions for answers to questions on DMCA notices, illegal file sharing, and copyright-related issues regarding electronic files.

FAQ Sections

General
Copyright & File Sharing
MIT Network
Risks of File Sharing

General

- **Q: What is peer-to-peer software?**
  A: Peer-to-peer (P2P) software is any file-sharing software that allows users to both share content from their computers and to connect to other, similarly configured computers for the purpose of downloading content. While P2P software has many legal uses, it is often used for unauthorized sharing and downloading of copyrighted materials such as music, films, video games and software.

- **Q: Can I use peer-to-peer applications such as Kazaa, Gnutella, Limewire, etc?**
  A: MIT does not prohibit the use of such applications on the network and recognizes the many legal benefits of P2P software. However, when using such applications, you must abide by the MITnet Rules of Use. Rule 4 ("Don't copy or misuse copyrighted material") is especially applicable in this case. Downloading copyrighted material, for which you have no license, is prohibited and is a violation of the Rules of Use. See the section below on Copyright & File Sharing as well as the Copyright Frequently Asked Questions.

- **Q: How should I configure my peer-to-peer applications?**
  A: Nearly all P2P applications have the ability to limit upload and download rates. We recommend you limit your application to use at most 5 KB/s for uploads (transfers from you to someone else) and 10KB/s for downloads (transfers from someone else to you). Please remember that the network is a shared resource, and academic use takes priority over downloading music.

  Some P2P applications allow you to specify what kind of connection to the Internet you have. We recommend you specify "Cable" or "DSL". This will ensure that your transfers do not hog the network and render it unusable for other students.

  Several applications (notably Kazaa) can function as a "Supernode" or "Ultrapeer". This functionality is enabled by default. When your computer is designated as a "Supernode" it means lots of other computers will try and connect to yours to transfer a file, rather than connecting to another machine. We ask that you disable the "Supernode" feature.

  Bittorent's download speeds are proportional to the amount of data you upload. Please be wary of your upload speeds and amounts. Bittorrent is not recommended for use in some older buildings that have not had recent network upgrades. It can quickly saturate the network causing you and your floormates to lose network connectivity.

  Finally, we ask that you close down P2P applications when not using them (such as when you go to class).

Copyright & File Sharing

If you don't find the answer to your question in this section, you can also refer to Copyright Frequently Asked Questions.

- **Q: What is the big issue with copyright and file sharing?**
  A: Many music, games, and videos downloaded through file-sharing programs fall into the category of copyright infringement. That is, the users downloading the files do not have the permission of the copyright owner. In addition, peer-to-peer file-sharing programs do not determine whether requests for media files are requests for copyright-licensed or freely-sharable materials. This means that if you copy music to your computer from a CD you purchased and are signed on to a peer-to-peer service with file-sharing enabled, you are making the copyrighted music you purchased available to others. YOU are distributing copyrighted material and the copyright owner can hold you liable for a copyright violation.

  The Digital Millennium Copyright Act (DMCA), enacted in 1998, makes it a crime to create, sell, or distribute software or other devices that can be used to illegally copy software. It also protects Internet Service Providers (ISPs) from liability for the transmission of infringing copyrighted materials if the ISP takes certain steps to notify the alleged infringer, and requires the ISPs to remove the infringing

materials.

Copyright owners frequently hire agents to scan university networks for copyrighted materials that are available to others including from computer systems on our network. MIT receives many notices from these organizations alleging copyright infringement. They focus on college campuses because of the high level of file-sharing activity. MIT is an ISP for many at the Institute who use campus network services such as MITnet.

- **Q: How can they see what I'm sharing?**
  A: Copyright holders have access to the same tools as you. P2P users can see the names of files, can access those files and find the IP address of the host sharing those files. This is all the information copyright holders need to serve notice to ISPs in violation. MIT uses the IP address of the host to identify the user registered to the machine involved. MIT does not disclose the user's identity to the copyright holders or their agents.

- **Q: What if someone else uses my machine to share copyrighted materials?**
  A: You are responsible for your computer and all activity that takes place on it. Be wary when lending your computer to others. You should also take necessary steps to ensure your operating system has the latest updates, patches, and virus software to best protect it from unwanted intruders and that it has a strong password.

- **Q: How can I legally download music?**
  A: There are many online services that allow for legal downloading of music. Some examples are iTunes, Napster, Rhapsody, plus many independent distributors. MIT does not recommend or endorse any one of these services over another. More information on legal alternatives for downloading music and movies can be found here.

- **Q: Does the DMCA make the use of peer-to-peer services illegal?**
  A: It is not against the law or campus policies to use peer-to-peer file-sharing programs or to swap materials that are not copyright-protected. It is against the rules to download and/or distribute copyright-protected material. If you are using a peer-to-peer file-sharing program, make sure that you are not "serving" copyright-protected materials to the world.

  Most file-sharing programs have worldwide file sharing turned on by default when they are installed. If you have copyright-protected materials on your computer, you need to disable file sharing so that the programs are no longer serving these materials from your computer. For information on disabling file sharing for the most popular P2P clients, visit The University of Chicago website.

MIT Network

- **Q: Will MIT IS&T scan my computer for unauthorized files?**
  A: No. MIT has little interest in repeating what the copyright holders are already doing. IT Security Services at MIT will monitor traffic patterns for the sole purpose of intrusion detection but does not "listen in" on network conversations. However, as detailed in the DMCA, MIT is required to take appropriate action when served a notice.

Risks of File Sharing

- **Q: Are there other risks associated with P2P?**
  A: Aside from being sued or subpoenaed, there are other good reasons to disable file sharing.
  Using some P2P applications will put you at risk of downloading files that contain viruses and trojans from a stranger's computer. Also, file-sharing sites often covertly package Spyware software that gathers personal information without your knowledge. This means that you may be giving hackers access to your personal files and programs or exposing your personal files to the outside world when you use file-sharing services. Use of file-sharing programs and inattention to sharing of personal information on your computer may lead to identity theft. You shouldn't trust the name of a file on a stranger's computer, or download an application from an untrustworthy source.