

Information: The Truth on Peer-to-Peer Networks

► Summary

"Peer-to-Peer" (or "P2P") networks are groups of computers with similar software programmed to communicate and share files with each other. They differ from other kinds of networks because they are not controlled by common "server" computers, and thus are essentially "peers."

There are different types and uses for P2P networks. [Wikipedia](#) is one good resource for learning [more about these networks and how they work](#). While there are valuable and convenient uses associated with P2P networks, users should be aware of security issues and the risks associated with sharing copyrighted material. Peer-to-peer network users should learn about these concerns before they participate, and children should get a parent or guardian's permission before start trading files on these networks.

► Content

Copyright Infringement

Among the most common uses of some P2P networks is the sharing of music, movies, software programs and other copyrighted material. If done without permission of the copyright holder or if not done for a lawful "fair use," this kind of sharing is illegal and can lead to serious liability.

Groups of copyright owners have filed lawsuits against some P2P network providers. These industry groups are the [Motion Picture Association of America](#) ("MPAA") and the [Recording Industry Association of America](#) ("RIAA"). The US Supreme Court has a case before it now to decide whether Grokster and other P2P networks like it are guilty of copyright infringement because of the file sharing done by users.

In recent months the RIAA and the MPAA have filed lawsuits against a number of P2P members who have made copyrighted files available for download over P2P networks. Thousands of individuals, have been sued across the country and also in other countries. RIAA and MPAA search P2P networks for files with copies of works they own. They identify the **Internet Protocol Address** of the person sharing or receiving, which is then recorded and used to track the person back through their Internet Service Provider (ISP). Once a lawsuit is filed, they then subpoena the records of the ISP to learn the identity of the user assigned that IP address.

Some ISPs have [raised questions with the courts](#) about the legality of the procedures used in some of these cases, but the RIAA and the MPAA have succeeded in forcing some providers to turn over the names and locations of some P2P users that have allegedly shared copyrighted material. Both groups have used this information to pursue potentially

costly infringement claims and some P2P users have had to pay thousands of dollars in damages.

If you want to learn more about this subject, you can visit:

<http://www.respectcopyrights.org/content.html>
<http://www.copyright.gov/circs/circ1.html>

which explain the positions of copyright holders. The websites of two advocacy groups that have opposed these suits are:

[Electronic Frontier Foundation](#)
[Electronic Privacy Information Center](#)

A few of the leading online websites for obtaining movies and music over the online are [Netflix](#) , [iTunes](#) , [Napster](#) , [MSN Music](#) , and [WalMart](#) .

Illegal Content

Many types of files can be shared through P2P networks. Some P2P users have downloaded or made available child pornography or other illegal data . By this point in this discussion, you realize that sharing P2P files does not provide the anonymity that some believe. You should be aware that storing some such files on your computer or trading them is a crime that can hold severe consequences.

Security Risks – Viruses and Spyware

Many programs that people use to access P2P networks contain potentially harmful features that are installed without the owner's knowledge. In many cases this includes Spyware and Adware. Many of the files available for download via P2P networks have been intentionally corrupted with viruses.

Spyware is a serious concern with some P2P network software. Spyware is software that provides others with information about a computer without the owner's knowledge or consent. Spyware can allow others to copy files without permission, redirect Internet browsers, monitor keystrokes, deliver pop-up ads and harm the performance of a computer and Internet service. Some anti-spyware programs will not remove spyware from P2P programs. To learn more about Spyware, visit [Webopedia](#) or [Wikipedia](#) .

P2P software can also include, or allow others to add computer viruses and Trojan horse programs to a user's computer. These can lead to some of the same effects as Spyware and can even allow a computer to be used remotely to send out large amounts of Spam

email. A computer with P2P software should always operate with a firewall and also with active anti-virus software. Make sure you know whether your program settings will affect how P2P software works.

Some users turn off the “sharing” feature of their P2P software as a way to avoid some of the problems the programs can cause. Not all P2P programs, however, will block all access into a computer when the sharing feature is off.