

The Perils of "Peer to Peer"

New technology with dangerous potential



[Libby Carty McNamee](#)

Richmond.com

Tuesday, March 01, 2005

Peer to peer file-sharing programs, often referred to as "P2P," are unique Internet network applications. Instead of utilizing the common model of a central server that controls and monitors the flow of data and information to consumers, these applications allow their users to independently share files amongst themselves. Users have direct access to other users' hard drives and faster file transfer since they are not going through a traditional server. Thus, users can use the Internet to freely exchange music, video and software files from their hard drive with each other.

In order to get started, each user must download and execute a peer-to-peer networking program, such as KaZaA, BearShare, Gnutella, and LimeWire. After launching the program, the new user can then enter the IP address of any other user who has downloaded the same software. Once the program finds that other user online, it will connect to that address and allow the new user to have open access that user's hard drive. However, the individual user has the option to choose how many P2P connections to open at one time. In addition, the user can designate files (s)he wishes to share publicly and those that (s)he wishes to protect with a password.

Although P2Ps offer some exciting opportunities in technology advancement, they are also fraught with potential abuse. Because the individual user becomes in effect his or her own server, there is a loss of control and no means to monitor appropriate bandwidth and security. For that reason most IT departments do not encourage the use of P2Ps. Users may expose themselves to identity theft, the nation's fastest growing crime, by unwittingly giving countless others access to the personal files stored on their computer. Furthermore, when a new user downloads a P2P program, (s)he can often inadvertently download viruses as well as spyware that operates on the computers by secretly amassing personal data that is often sold.

Another potential danger of P2Ps is copyright infringement. By file sharing, users may attempt to avoid payment to the artist. P2P has become synonymous with the application Napster, the site that allows music fans to download software and share music files with one another. The recipients were able to avoid the "middleman" and access the music, CDs, and DVDs for free. A number of record companies have sued users for illegal

sharing of copyrighted content.

The U.S. Supreme Court has agreed to hear *MGM v. Grokster* on March 29, 2005, which raises thorny issues regarding P2P file-sharing systems. In this case twenty-eight of the world's largest entertainment companies have filed suit against the programs of Morpheus, Grokster, and KaZaA. They are attempting to hold these producers of file-sharing programs liable for the infringements committed by their users in illegally downloading copyrighted movies and music without paying for them.

Another serious concern is the open exchange of child pornography as well as pornography in general. Since there is no common server, P2Ps make it easier for people to exchange pornographic images and videos without detection from the authorities. Although many parents utilize filtering systems on their computers, they are far from foolproof. Furthermore, some P2P services are adding an encryption feature that will make it even more difficult for law enforcement officials to investigate. While searching for and downloading images on P2P networks such as movies and digital music, there is a significant risk that young users may inadvertently expose themselves to pornography.

Recently the nationwide Internet Crimes Against Children Task Force (ICAC) conducted a sting operation that targeted the growing phenomenon of child pornography trading through P2P programs.

The first phase yielded 7,500 cases, 148 of which were located in Virginia. Former Attorney General Jerry Kilgore and his successor Judy Jagdmann have been working to investigate and prosecute those cases throughout the Commonwealth.

Noting the potential dangers of the P2P programs, Kilgore recently sent a letter to the major P2P sharing companies in which 48 fellow Attorney Generals joined. The letter questioned the companies' failure to provide consumers with the full information necessary for them to make informed decisions about file sharing technology and the potential dangers associated with its use. According to Richard Campbell, Deputy Attorney General for Technology and Transportation, P2P "is a reality of life nowadays. Citizens, and particularly parents, need to be aware of the hazards of Identity Theft, exposure to obscene material and copyright infringement that P2P ushers into their homes by way of the computer. The information age brings with it great changes and exponential access to entertainment, but we have to be careful to walk wisely in making those strides."

The Federal Trade Commission (FTC) has become increasingly concerned with the problems associated with P2Ps due to increasing consumer complaints about increased exposure to spyware, viruses, copyright infringement, security, and undesired pornography. Many consumers are unaware that it is illegal to download copyrighted files even if they are paying a fee to use premium P2P software. In coordination with the FTC, many of the P2Ps are now issuing a "cybersafety" initiative that includes a series of consumer advisories on these issues.

Libby Carty McNamee is a lawyer and freelance writer living in the Richmond area. She can be contacted at libbymcnamee@yahoo.com and 804-378-8218. This article does not constitute legal advice. If you need legal assistance, please contact a lawyer.