

This article was originally published in the December 2008 issue of New Jersey Lawyer Magazine, a publication of the New Jersey State Bar Association, and is reprinted here with permission.

Cybercrimes

File-sharing Programs Violating Copyright and Child Pornography Distribution Laws

by **Darren Gelber**

The proliferation and popularity of peer-to-peer (P2P) software programs has the potential to unwittingly expose users to arrest and prosecution for offenses they never even knew they were committing.

Simplly described, P2P programs, such as Gnutella, Kazaa, Limewire, or eMule with Kademia, allow those who download the free software to use the Internet to search through the computers of other users for files they would like to copy to their own computers. Typically, the files are downloaded by the P2P user into a folder named "My Shared Files." These files could be digital photographs, digital music, video clips or any other form of computer file.

Once a user finds a file on someone else's computer in the "My Shared Files" folder that is of interest, a simple mouse click transfers a copy from the other person's computer to the user's hard drive, and then into the user's "My Shared Files" folder. By default, P2P programs are set so that anything in a user's "My Shared Files" folder is available to anyone else on the P2P network.

Users who partake in these P2P file-sharing programs run the risk of violating copyright laws when they knowingly trade and transfer copyrighted material, but that is not the focus of this article. This article is intended to educate the unwary user, and his or her counsel, about how using these types of programs can potentially expose the user to allegations of other types of criminal activity.

For example, New Jersey's distribution of child pornography statute¹ provides that:

Any person who knowingly receives for the purpose of selling or who knowingly sells, procures, manufactures, *gives, provides,* lends, trades, mails, delivers, *transfers,* publishes, *distributes, cir-*

culates, disseminates, presents, exhibits, advertises, offers or agrees to offer, through any means, including the Internet, any photograph, film, videotape, computer program or file, video game or any other reproduction or reconstruction which depicts a child engaging in a prohibited sexual act or in the simulation of such an act, is guilty of a crime of the second degree. [emphasis supplied].

A violation of this statute is punishable by up to 10 years in prison. By contrast, merely possessing child pornography is a fourth-degree offense, punishable by up to 18 months in prison.²

There are many reputable public sources that have commented upon the dangers inherent in P2P software and have warned that setting up these networks may lead to subscribers unwittingly engaging in criminal acts, or in criminal acts far more serious than users may anticipate. For example, in an Aug. 5, 2004, letter addressed to an association of P2P networks, the National Association of Attorneys General, including as a signatory then-New Jersey Attorney General Peter Harvey, warned:

P2P file-sharing technology can allow its users to access the files of other users, even when the computer is "off" if the computer itself is connected to the Internet via broadband. P2P users, including both home users and small businesses, who do not properly understand this software have *inadvertently* given other P2P users access to tax returns, medical files, financial records, personal e-mail, and confidential documents stored on

their computers. Combating identity theft is one of our priorities, and many of our States have enacted laws to stop it. Consequently, P2P users need to be properly educated so that they will not inadvertently share personal files on their hard drives with other users of your P2P file-sharing technology.

In an FTC consumer alert published by the Federal Trade Commission (FTC) in 2003, the federal agency charged with protecting the nation's consumers warned that "file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you *may unknowingly* allow others to copy private files you never intended to share." More superficially, the FTC offered the following cautions:

- Set up the file-sharing software very carefully. 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 also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.
- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or broadband connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These 'always on' connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

The Federal Bureau of Investigation

has echoed these warnings: "if Peer-to-Peer software is not properly configured, you may be *unknowingly* opening up the contents of your entire hard drive for others to see and download your private information."

The principles expressed in these authoritative publications as applied to users of pornographic images and video clips are exemplified in commentary contained in a May 4, 2004, letter to the FTC from five respected United States senators. The letter presciently predicted a scenario that has actually confronted unwary individuals who download pornographic material for their own viewing:

"viral" redistribution³ of *any* pornography can endanger not only children, but also *adults who want to view adult pornography*. For example, imagine a college student, who uses file-sharing software as intended to download for private use a violent adult pornographic image. Automatically, however, the P2P program itself makes the image accessible for downloading by every other user of the file-sharing software, including children or users who live in different areas of the country with different community standards. As a result, this student may redistribute violent pornography to children and others – and risk criminal prosecution under state or federal criminal laws governing pornography distribution. Both Congress and the Department of Justice have advised prosecutors to target obscenity prosecutions toward pornography *distributors* – particularly those who distribute to minors.

Unfortunately, this is no hypothetical. It is happening now. Otherwise law-abiding adults who may only have meant to view pornography privately are—intentionally, negligently or unknowingly—becoming pornography distributors who distribute world-wide,

to children and adults. We doubt that most such adults realize how "viral" redistribution of *any* pornography endangers both adults and children.

Thus, imagine a scenario in which a person knowingly possessed child pornography by using P2P software to download images of a child engaged in a prohibited sexual act (a fourth-degree offense). Once that file is downloaded onto the user's hard drive into the "My Shared Files" folder using P2P software, by default it becomes available to other users of the P2P network, turning someone who thought he was *possessing* child pornography into someone who *distributes* child pornography—a much more serious offense. An investigator can simply log onto a P2P network, search for illegal images or videos on the hard drives of other P2P users, and then transfer a copy to the investigator's hard drive. Once that transfer is complete, the owner of the source computer has just transferred or distributed child pornography unknowingly, expanding his or her potential prison term.

Courts considering this issue have not been sympathetic to the plight of defendants who claim they never intended to distribute the child pornography located on their computer. For example, in *State v. Tome*,⁴ the Appellate Division upheld the conviction of a defendant for distribution of child pornography, finding that by using a P2P program to download pornography, and knowing that other P2P users could access what had been downloaded onto his computer, he had offered the illegal images to others, and thus was guilty of the distribution charge.

In *United States v. Shaffer*,⁵ the United States Court of Appeals for the Tenth Circuit held that a defendant distributes child pornography by making computer files containing child pornography available for others to download. Similarly, the Court of Appeals for the Seventh Circuit

held, in *United States v. Carani*,⁶ that it was proper for the district court to reject the defendant's claim that he "had never intentionally distributed child pornography, but that he may have done so inadvertently through the Kazaa program as he did not understand what the 'My Shared Folder' did," because the defendant knowingly made the images available to others through the Kazaa network (a P2P network). The Fifth and Eighth circuits have come to similar conclusions.⁷

The use that P2P networks were designed to meet—the sharing of digital files—is in and of itself dangerous, as it exposes users to copyright infringement claims. What users may not know is that use of these programs may magnify their illegal conduct into something far more serious than they ever imagined, especially where images and videos of child pornography are involved. ⚡

Endnotes

1. N.J.S.A. 2C:24-4b(5)(a).
2. See N.J.S.A. 2C:43-6a(2); 2C:43-6a(4).
3. The senators' letter observes that P2P software enables "so-called 'viral' redistribution: By default, users of the software make all files downloaded available for redistribution to other users. This 'viral' redistribution can thwart enforcement of the rights of artists because one infringing copy of a popular work can quickly multiply over a network. 'Viral' redistribution works by turning mere consumers of content into international distributors of content. As a result, people seeking content to use at home can inadvertently incur all the complex and unfamiliar risks of managing an international content-distribution operation."
4. 2007 WL 1135690, A-4283-05T1 (App. Div. April 18, 2007) (unpublished), *certif. den.*, 192 N.J. 74 (2007).
5. 472 F.3d 1219 (10th Cir. 2007).
6. 492 F.3d 867 (11th Cir. 2007), *cert.*

denied, __U.S. __, 128 S. Ct. 932, 169 L. Ed. 2d 769 (2008).

7. See *United States v. Todd*, 100 Fed. Appx. 248, 2004 WL 1240521 (5th Cir. 2004), *cert. granted and vacated on other grounds*, 543 U.S. 1108 (2005); *United States v. Griffin*, 482 F.3d 1008 (8th Cir. 2007).

Darren Gelber, a certified criminal trial attorney, is co-chair of the criminal law and civil rights group at Wilentz, Goldman & Spitzer in Woodbridge. He represents clients in federal and state courts, and in appellate and administrative matters.