Testimony of

Mr. John Malcolm

September 9, 2003

Statement of John Malcolm
Deputy Assistant Attorney General
Criminal Division

Before the Committee on the Judiciary
United States Senate

Regarding Peer-to-Peer Networks and Child Pornography

September 9, 2003

Mr. Chairman, Senator Leahy, and distinguished Members of the Committee, thank you for inviting me to testify before you today on this critical topic. The sexual abuse of a child is a horrific act, and this horror is often exacerbated by pedophiles who memorialize their repugnant crimes in photographs and videos. Sadly, with increasing frequency, such offenders are choosing to disseminate these grotesque memorials to millions of people over the Internet with a few clicks of a computer mouse.

The exploitation of children through the production and dissemination of child pornography is an intolerable evil that we must work to obliterate. Toward that end, Congress recently made significant strides by enacting the PROTECT Act, which provides invaluable tools to law enforcement to aggressively prosecute crimes involving the scourge of child pornography. Nevertheless, child pornographers continue to find ways to employ the ever-evolving technology of the Internet and computers to commit their deviant crimes. In turn, law enforcement must respond to technological advances, as well, eradicating child pornographers from every forum in which they lurk, be that in cyberspace or otherwise. Thus, I commend you for holding this hearing. I hope to provide you with an understanding of how peer-to-peer file-sharing computer networks are being used to distribute and receive child pornography, how pornography in general is being made available to children over peer-to-peer networks, and how the Department of Justice is attempting to root out those who are taking advantage of technology to distribute child pornography.

At the outset, it is important to acknowledge the Department's firm belief in the positive aspects of the Internet. In too many instances, people view government officials, especially those who work in federal law enforcement, as anti-technology -- intent only on stifling the growth of technology and the Internet. This is simply not the case. The Internet's benefits are too numerous and obvious to restate here, and the Department of Justice supports the full development of the Internet and technology. But, just as law enforcement must operate in a way that does not unnecessarily impede the advancement of technology, so too must people acknowledge that technology is often misused to perpetrate criminal activity which can, in and of itself, undermine public confidence in those technologies and impede their advancement.

Before I address the Department of Justice's approach to the proliferation of child pornography over peer-to-peer file-sharing networks, let me first describe how these so-called "P2P" networks operate. From this common understanding of the technology, we can see how P2P networks are being abused by child pornographers, the unique issues that arise in regard to criminal prosecutions involving P2P networks, and how the use of P2P networks to disseminate child pornography fits into the greater context of child pornography crimes being committed on the Internet.

BACKGROUND ON PEER-TO-PEER FILE-SHARING NETWORKS

First let me contrast peer-to-peer networks with the more traditional network that is used to share computer files. On traditional networks, people who want to share files -- including contraband files -- store them on one or more central "servers," which are powerful computers that supply the files to a number of smaller, less powerful computers such as the computer you might have at your desk. Picture a bicycle wheel, where the server computer is the hub that sends files out through the spokes to smaller computers arrayed along

the tire. A file that is available on one customer's desktop is not available to any other computer on the network until it is uploaded to the central server.

The peer-to-peer network, by contrast, is less centralized; in fact, it is fluid by design. If a traditional network looks like a bicycle wheel, a peer-to-peer network looks like a fisherman's net. Each peer computer is connected to the rest of the peer computers either directly or through one or more intermediary computers. In a P2P network, files are kept not on a central server but, rather, on each of the peer computers hooked into the network at any given point in time.

Any peer computer, which could be the computer sitting on your child's desktop, can be utilized to download P2P software from the Internet and thereby gain access to shared files located on other computers connected to that network. Once the software is installed, P2P networks can be accessed to transfer virtually anything that can be put into digital format, including pictures, music, or videos. A user may search the P2P network for files based on certain characteristics such as a keyword or file name, for example, and may narrow his or her search to identify only video files, images or audio files. The P2P software then displays a list of shared files matching the search criteria that are currently available from other computers connected to the network. Once the user selects those files that he wishes to download, the source and destination peer computers exchange files directly. Similarly, a user may also elect to share certain files on his own computer with other users on the P2P network. Given this format, it is not surprising that this medium has become a hotbed of criminal activity, particularly where child pornography is concerned.

POTENTIAL FOR CRIMINAL ACTIVITY THROUGH USE OF PEER-TO-PEER FILE-SHARING NETWORKS

The potential for criminal activity through the use of peer-to-peer networks is no secret to the members of this Committee. The possibilities include privacy and security intrusions; copyright infringement; the dissemination of adult pornography to children; and, as underscored by this hearing, the distribution of child pornography.

Privacy and Security Intrusions

Peer-to-peer file-sharing software is associated with three types of potential privacy or security intrusions. The first potential intrusion comes when a user installs the peer-to-peer software on his computer. Some P2P software is intentionally infected by adware, spyware, and even viruses or so-called "Trojan horses," which are applications that appear benign but contain latent viruses. Thus, merely installing P2P software can expose a peer computer to attack. The next type of intrusion may occur when the user tells the P2P software what files to share. P2P users have inadvertently given other people access to their tax returns, medical files, financial records, personal e-mail, and confidential legal documents such as attorney-client communications. The final type of intrusion may occur once the user starts sharing files with others. Hackers have exploited the openness of P2P networks to propagate viruses, worms, and other malicious computer software. Sadly, but predictably, at least one virus propagated itself over a peer-to-peer network in part by renaming itself as computer files that promised pornographic images. This combination of vulnerabilities makes using a peer-to-peer file-sharing network a very risky proposition indeed.

Copyright Infringement

At this point there should be no doubt that even if P2P networks can be used for legitimate purposes, a large number of people are using P2P networks for copyright infringement. Given how P2P networks operate, it is easy to see why. P2P networks involve millions of users, and because they are increasingly fast, users can download files with relatively little risk of detection. The Department of Justice will fight copyright infringement in any medium in which it takes place, and I have therefore specifically directed the Department's Computer Crime and Intellectual Property Section to consider means for combating copyright infringement over P2P networks.

Distribution of Adult Pornography that is Legal, But Easily Seen by Children

Congress is well aware that adult pornography is readily available to children on the World Wide Web and is often inadvertently accessed by children using innocuous search terms, such as the names of cartoon characters or children's television shows. Indeed, to combat this growing problem, Congress, through the PROTECT Act, recently enacted a law criminalizing the use of domain names that mislead minors into viewing harmful material.

Despite the potency of this new legislation, it does not extend to file names that individuals create for files on their computers that they choose to share over P2P networks. Thus, any child who downloads P2P

software and enters an innocuous search term may be confronted with files containing adult pornography that have been given misleading names. On a positive note, most P2P software packages contain filters that can be activated to screen out adult material and/or digital images, and many of these filters are password protected, so that children cannot deactivate filters that their parents have activated.

Distribution of Child Pornography

Like all other Internet venues, P2P networks are fertile ground for the distribution and receipt of child pornography. The design of P2P networks allows perpetrators readily to identify numerous desired files on other users' computers using fairly blatant search terms, such as "child porn" or "lolita." Users can then download materials relatively quickly for their personal possession and use and retreat into obscurity.

LAW ENFORCEMENT ISSUES UNIQUE TO PEER-TO-PEER NETWORKS

Because peer-to-peer networks operate as a diffuse community of computers, the investigation of child pornography offenses in the peer-to-peer context requires a proactive and focused approach by law enforcement. The lack of a central server means that there is no clearinghouse for files and information that can serve as a bottleneck or choke point where law enforcement can gather logged evidence of illegal activity and cut off the supply of contraband files. Moreover, the decentralized nature of P2P networks means that there is no central community where people communicate regarding their illegal plans. Instead, peer-to-peer file-sharing networks are diffuse in nature: millions of people can join loosely-knit groups without the need for humans to communicate at all, since their computers will automatically handle all of the details for them. The only entrance fee to an illegal group is the time to download P2P software, boot it up, and start uploading and downloading files.

Relative Anonymity

As compared with Internet access in general or email accounts, many P2P networks do not require individual users to set up an account with a central authority. P2P users can create and change user names at will, and user names rarely contain any information that would reveal the true identity of the user. Nevertheless, just as an individual cannot receive or place a telephone call without a telephone number, every instance of Internet access is associated with in internet protocol, or "IP," address. Thus, using P2P software, a law enforcement agent can identify a file containing child pornography, and while downloading that file, identify the IP address of the computer sending it. The agent can then determine which Internet service provider owns that IP address, and serve legal process on that Internet service provider to obtain the name and address of the P2P user associated with that IP address on the date and time that the file was shared. Moreover, seizure of that user's computer will often reveal the IP addresses of other computers with which contraband files were shared. Thus, although it is true that absent an undercover operation, there is relatively little risk of detection on P2P networks, no P2P user is truly "anonymous."

Notably, however, new generations of P2P file-sharing protocols and tools are promising their users even more anonymity, such as by hiding IP addresses behind proxy servers or even refusing to recognize preliminary inquiries from computers known to be associated with law enforcement. Some peer-to-peer tools are even touting their ability to shield users from the view of victims or law enforcement. Should this technology come to fruition, it will present significant challenges to law enforcement and will undoubtedly make P2P an even more popular vehicle for trading child pornography.

THE DEPARTMENT OF JUSTICE'S EFFORTS CONCERNING THE DISTRIBUTION OF CHILD PORNOGRAPHY OVER PEER-TO-PEER NETWORKS

The Department of Justice is committed to vigorously prosecuting child pornography in every forum in which it appears, including the myriad channels of access available on the Internet. Certainly, P2P networks are of significant law enforcement concern and focus, particularly because of their decentralized design and relative accessibility and ease of use. The Department has established a High Tech Investigative Unit within the Child Exploitation and Obscenity Section dedicated to providing investigative support in prosecutions for crimes involving child exploitation and obscenity, and specifically, child pornography on the Internet, including in P2P networks. Consistent with the Department's mission to eradicate child pornography, the Federal Bureau of Investigation is currently considering a protocol for investigating child pornography cases in the relatively new area of P2P technology.

While there is no question that there is a plethora of pornographic and obscene material on P2P networks, which is easily accessible by children, it is difficult to quantify what percentage of the dissemination of child pornography on the Internet occurs via P2P networks. The General Accounting Office ("GAO")

report released on March 13, 2003 indicates that, while reports on P2Ps have increased, ultimately only 1 percent of the tips from the public received by the National Center for Missing and Exploited Children since 1998 involved P2P technology.

There are several other avenues of Internet communication that, for a number of reasons, currently hold significant appeal for purveyors and seekers of child pornography. Among the most popular of these are commercial web sites, newsgroups, and internet relay chats, or "IRCs."

Arguably the most troublesome of these are commercial web sites. Even greater than the percentage of the computer-literate population that has ever utilized P2P software is the percentage of people who have utilized web sites; indeed, nearly everyone old enough to type words on a computer keyboard understands how to "surf the web" and access websites on topics of interest. Computers are sold with Internet browser software pre-installed. Capitalizing on the accessibility and commensurate popularity of the Web, child pornographers offer images and video files for sale on a vast number of commercial websites hosted on servers throughout the world. These websites often boast "extreme" and varied material, for which child pornographers typically have a seemingly insatiable desire. The increasing demand drives the market for child pornography on the Web. As a result, the financial profits associated with the exploitation of children through such sites can be staggering. Undercover purchases and the utilization of legal process to obtain credit card and billing records can lead to extensive investigations and prosecutions in these types of cases.

Slightly more savvy computer users utilize IRCs to obtain child pornography. Through IRCs, individuals communicate in real time with other users currently online. Such users can advertise the files that they possess on their computers, and invite others to download those files for a price. A typical user will set up "rules" for access to his file collection. Thus, for example, a user will allow another user to download 5 images only if that person first uploads 3 images. A user may further specify that he only wants pictures of "girls under 10" or "father-son incest." Many times, the user sets his computer to scan uploaded images to ensure that the images he is receiving are not duplicative of those already in his collection. The user may also threaten to ban individuals from future trading if they do not abide by his rules, for example, by uploading inauthentic images. Sometimes, users offer a "free look" at small files to entice others to trade. Once a user identifies a desirable potential source of new files, the donor and recipient go into a "private" window and their computers communicate directly to facilitate the downloading and uploading of images. Using IRCs, a child pornographer can increase the size and diversity of his collection, which collectors of child pornography characteristically and compulsively seek to do. By contrast, offering files on P2P does not automatically result in receiving files in return, making it a less appealing prospect. IRC users can be targeted through undercover operations, just as P2P users can, with one added benefit: because IRCs operate through centralized servers, the service providers frequently retain records of communications, albeit for short periods of time, which can be obtained through legal process.

Perhaps the most popular aspect of Internet use is communication via email; only marginally more technical than email are newsgroups. By joining newsgroups dedicated to a given subject matter, users can communicate by email with like-minded individuals regarding their common interests. Thus, there are newsgroups dedicated to football, cooking, astronomy, and - - not surprisingly - - child pornography. Newsgroups are attractive to child pornographers because, like IRCs, they precipitate trading relationships. Law enforcement can target newsgroups through undercover trading and subsequent use of subpoenas or court orders for the records of internet service providers.

CONCLUSION

It is my hope that I have provided the Committee with a clearer understanding of peer-to-peer technology, its implications for the dissemination of child pornography, and where it fits into the larger context of the proliferation of child pornography on the Internet. Most assuredly, the Department of Justice is committed to eradicating child pornography in every possible venue through an aggressive prosecution strategy.

Mr. Chairman, I again thank you and the Committee for the opportunity to speak to you today, and I would be pleased to answer any questions the Committee might have.