G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

November 14, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate

Subject: *Posthearing Questions from the September 9, 2003, Hearing on "Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks"*

Dear Mr. Chairman:

This letter responds to your September 17, 2003, request that we provide answers to questions relating to our September 9, 2003, testimony.[1] In that testimony, we discussed the availability of child pornography on peer-to-peer (P2P) networks. The questions posed by Senator John Cornyn and Senator Patrick Leahy to GAO, along with our responses, follow.

1. *Could you provide examples or data regarding potentially positive uses of P2P technology?*

Among the major uses of peer-to-peer technology are the following:

- *File sharing*, which includes applications such as Napster and KaZaA, along with commercial applications such as NextPage.[2] File-sharing applications work by making selected files on a user's computer available for upload by anyone else using similar software, which in turn gives the user access to selected files on the computers of other users on the peer-to-peer network.
- *Instant messaging (IM)*, which includes applications that enable online users to communicate immediately through text messages. IM promotes a two-way conversational style of communication with minimal delay. Commercial vendors such as America Online (AOL), Microsoft, and Jabber offer free IM tools.

[1] U.S. General Accounting Office, *File-Sharing Programs: Users of Peer-to-Peer Networks Can Readily Access Child Pornography*, GAO-03-1115T (Washington, D.C.: Sept. 9, 2003).

[2]NextPage provides information-intensive corporations with customized peer-to-peer file-sharing networks. It enables users to manage, access, and exchange content across distributed servers on intranets and via the Internet.

- *Distributed computing*, which includes applications that use the idle processing power of many computers. For example, the University of California–Berkeley's SETI@home project uses the idle time on volunteers' computers to analyze radio signal data. By taking advantage of the unused resources on volunteers' computers, the SETI@home project has been able to obtain more processing power than that available from the most powerful supercomputer for about 2 percent of the cost.

- *Collaboration applications*, which enable teams in different geographic areas to work together and increase productivity. Collaboration applications often combine single-function peer-to-peer applications, like IM and file sharing, into more complex applications. For example, the Groove application can access data on traditional corporate networks and on nontraditional devices such as personal digital assistants (PDAs) and handheld devices. This application offers IM, Web connectivity, and other add-on services.

2. *To what extent are P2P software sellers able to track individuals who use their software?*

The ability of peer-to-peer software vendors to track or regulate the use of their software depends on whether the peer-to-peer network is based on a centralized model, such as that used by Napster, or a decentralized model, such as the Gnutella[3] network used by KaZaA. In the centralized model, which is based on a central server or broker that directs traffic between individual registered users, it is possible for the administrators of the central server to track some of the individuals' activities by monitoring their interactions with the central server or database. In the decentralized model, in which individuals find and interact directly with each other, the ability of peer-to-peer software vendors to track individuals who use their software is greatly diminished. Any user of a decentralized peer-to-peer network, including the vendors of the software, can search the network to determine the files that are being shared on the network. However, according to one major software vendor, vendors of file-sharing software have no special ability to track or regulate the actions of the users of the software.[4]

3. *Are there any reasons why child pornography may be underreported on peer-to-peer networks?*

---

[3]According to LimeWire LLC, the developer of a popular file-sharing program, Gnutella was originally designed by Nullsoft, a subsidiary of America Online (AOL). The development of the Gnutella protocol was halted by AOL management shortly after the protocol was made available to the public. Using downloads, programmers reverse-engineered the software and created their own Gnutella software packages.

[4] Statement of Mr. Alan Morris, Executive Vice President, Sharman Networks Limited, before the Senate Judiciary Committee regarding "Pornography, Technology and Process: Problems and Solutions on Peer-to-Peer Networks" (Washington, D.C.: Sept. 9, 2003).

We do not know if the volume of child pornography on peer-to-peer networks is underreported. In our testimony, we cited the number of reports or tips received by the National Center for Missing and Exploited Children (NCMEC) as one indication of the volume of child pornography on peer-to-peer networks and on the Internet in general. NCMEC, a federally funded nonprofit organization that serves as a national resource center for information related to crimes against children, operates a CyberTipline that receives child pornography tips provided by the public; its CyberTipline II receives tips from Internet service providers. The Exploited Child Unit investigates and processes tips to determine if the images in question constitute a violation of child pornography laws and provides investigative leads to the Federal Bureau of Investigation (FBI), U.S. Customs, the Postal Inspection Service, and state and local law enforcement agencies.

As shown in table 1, in 2003 the NCMEC CyberTiplines received over 62,000 Internet-related reports of child pornography. Of these, 840, or about 1.4 percent, were related to peer-to-peer networks. However, we do not know if the number of reports received by NCMEC accurately reflects the volume of child pornography on peer-to-peer networks or on the Internet in general, since the reports are based on tips that the public or system users submit rather than a systematic analysis of network content.

Table 1: NCMEC CyberTipline (Internet-Related) Referrals to Law Enforcement Agencies, Fiscal Years 1998–2003

	Number of tips					
Technology	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**
Web sites	1,393	3,830	10,629	18,052	26,759	45,035
E-mail	117	165	120	1,128	6,245	12,403
Peer-to-peer	—	—	—	156	757	840
Usenet newsgroups & bulletin boards	531	987	731	990	993	1,128
Unknown	90	258	260	430	612	1,692
Chat rooms	155	256	176	125	234	786
Instant Messaging	27	47	50	80	53	472
File transfer protocol	25	26	58	64	23	13
Total	**2,338**	**5,569**	**12,024**	**21,025**	**35,676**	**62,369**

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

4. *Is there something particularly dangerous about the pornography on peer-to-peer networks, either in the user's ability to share it anonymously or in its accessibility to children?*

The pornography available on peer-to-peer networks is not necessarily more dangerous than the pornography available on Web sites or through other electronic means of dissemination. Although some users of peer-to-peer networks might believe that they are sharing files anonymously, it is possible for law enforcement officials to discover the

identities of individuals sharing child pornography and other illegal material on peer-to-peer networks. With peer-to-peer networks, pornography is easily accessible to children and the risk of inadvertent exposure to pornography is significant. However, pornography is also easily accessible through other electronic means, such as Web sites, and the risk of children's inadvertent exposure to pornography exists on these other mediums as well.

5. *What steps does it take to keep child pornography off a peer-to-peer network?*

Preventing the introduction of child pornography on a peer-to-peer network would be very difficult, but legal means exist to investigate and prosecute those sharing this material on the network. Unlike traditional Web sites, which have centralized content management, users control the content that is available on peer-to-peer networks, and the users of the network are constantly in flux. Nonetheless, law enforcement agencies can search peer-to-peer networks for child pornography and investigate reports of illegal material submitted to the NCMEC and other agencies. Once child pornography files are identified on a peer-to-peer network, legal mechanisms can be used to identify, investigate, and prosecute the individuals sharing the illegal files.

6. The "fair use" doctrine of copyright law gives consumers a certain amount of flexibility to use copyrighted materials they legitimately possess, without risk of liability for copyright infringement. Does that doctrine apply, however, to materials that have yet to even be released to the public? Under what conditions, if any, would it even be possible for ordinary consumers to lawfully possess such "pre-release" materials? Should the NET Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), be amended, so that any *reproduction or distribution of "pre-release" material shall constitute per se infringement under 17 U.S.C. 506(a)(2)?*

The doctrine of fair use can apply to unreleased material. The fair use doctrine, which has been codified at 17 U.S.C. § 107, is available as an affirmative defense to those who infringe on copyrighted works that have yet to be released to the public. In order to respond to your question, we have interpreted your term "released," which is not defined under copyright law, to be equivalent to the term "published" under these laws. Although an infringing use of an unpublished work is less likely to be deemed fair by the courts, Congress amended the statutory codification of the fair use doctrine in 1992 to make explicit that the fact that a work is unpublished shall not itself bar a finding of fair use.

Under copyright law, it is not only possible but also plausible that a consumer could lawfully possess "pre-release" materials. For example, software developers frequently distribute "beta" versions of software programs for the purpose of "debugging" before the release of the program for retail sale. Any individual that the copyright holder intended to receive a work for a limited purpose would have a lawful right to its possession,

notwithstanding that the material had not been released for sale to the general public. The subsequent distribution of such a work from an intended recipient might breach the terms the copyright holder set, if any, and could subject the recipient to civil and criminal penalties under copyright laws.

Our work on peer-to-peer networks did not address issues concerning pre-release materials, and therefore we are unable to provide an opinion on the merits of amending the No Electronic Theft (NET) Act. We note, however, that the act's criminal penalties apply to all copyrighted works, regardless of whether they have been released to the public, and civil and statutory damages, up to $150,000 per infringement of a registered work, remain available to copyright holders regardless of whether the infringed work has been published or released (17 U.S.C. § 504). Further, in order to satisfy the threshold for a criminal infringement, the infringement must involve at least one copy, and the value of the total infringement must exceed $1,000 within a 180-day period (17 U.S.C. § 506). We understand that Senators Cornyn and Feinstein recently introduced legislation proposing to remove this threshold for criminal infringement.

In responding to these questions, we relied primarily on past work. We assessed the major uses of peer-to-peer technology, examined methods available to track the users of peer-to-peer applications, and reviewed the feasibility of controlling the content available on peer-to-peer networks. We also obtained updated information regarding the number of Internet-related Cybertipline referrals from the NCMEC. Finally, we reviewed and analyzed the applicability of the fair use doctrine of copyright law to pre-release copyrighted material.

Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6240 or Mike Dolak, Assistant Director, at (202) 512-6362. We can also be reached by e-mail at koontzl@gao.gov and dolakm@gao.gov, respectively. Key contributors to this correspondence include Jason B. Bakelar and Lori D. Martinez.

Sincerely yours,

Linda D. Koontz
Director, Information Management Issues

(310392)