Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C.

In the Matter of	
	WC Docket No. 07-52
Broadband Industry Practices	

REPLY COMMENTS OF CHRISTIAN COALITION OF AMERICA, THE CP80 FOUNDATION, ENOUGH IS ENOUGH, AND STOP CHILD PREDATORS

These reply comments to comments of Free Press, *et al*., dated Feb. 13, 2008 are submitted on behalf of a coalition of national, non-profit organizations broadly representing the interests of parents, children, and law enforcement officers. Coalition members[1] share a commitment to the effective enforcement of the law – in particular prohibitions against child pornography, obscenity, and other predatory behavior against children. The coalition is concerned that approval of the Vuze and Free Press petitions[2] might make it more difficult for Internet Service Providers (ISPs) to monitor and filter the use of anonymous and decentralized peer-to-peer (P2P) networks to facilitate crimes against children, and to report those crimes to authorities.

If the Federal Communications Commission issues rules clarifying what practices constitute "reasonable network management" under the *Broadband Policy Statement* (*Statement*), it should state expressly and unequivocally that ISPs may monitor for the

[1] The coalition consists of Christian Coalition of America, the CP80 Foundation, Enough is Enough, and Stop Child Predators (collectively the "coalition").

[2] *See* Free Press, *et al.*, Petition for Declaratory Ruling, WC Docket No. 07-52, Nov. 1, 2007 (Free Press Petition); and Vuze, Inc. Petition for Rulemaking to Establish Rules Governing Network Management Practices By Broadband Network Operators, WC Docket No. 07-52, Nov. 14, 2007 (Vuze Petition).

transmission of child pornography and other illegal content,[3] may filter such content, and may report such content to authorities.

After discussing predators' use of P2P technology to access child pornography and the invaluable role ISPs have played in combating child exploitation, this filing offers three reasons for such a rule. First, the *Statement* already implies that network operators are entitled to filter and report illicit content. Second, enabling ISPs to filter illegal materials will help reduce the amount of child pornography transmitted over their networks. Third, the rule would preserve the ability of ISPs to assist law enforcement officials in investigating Internet crimes.

The Commission should not stop at stating expressly that ISPs are entitled to actively search their networks for illicit materials. It also should acknowledge the reality of how computer crimes are actually uncovered. Sometimes ISPs discover evidence of criminal activity because they are looking for it. But sometimes they come across it in the course of routine network management. The Commission must take care not to issue rules that, by limiting the flexibility ISPs currently enjoy in managing their networks, could inadvertently reduce ISPs' opportunities to unearth illegal conduct.

I. P2P Networks Are Routinely Used to Facilitate Child Exploitation.

It is undeniable that the Internet has revolutionized the way Americans communicate. Yet not all of those changes are to be applauded. Like any neutral technology, the Internet is susceptible to abuse. Some of the most depraved abuses are perpetrated by "highly organized and technologically sophisticated groups of pedophiles who utilize advanced technology to . . .

[3] The coalition believes that political and religious speech always constitute "lawful Internet content" within the meaning of the *Statement*. Its members would oppose any efforts to filter such expression.

sexually exploit and abuse children."[4] The problem is as widespread as it is dire. In the decade since the FBI in 1996 launched an initiative to combat online child pornography and exploitation, the number of such cases jumped by 2,050 percent, from 113 to 2,500. The FBI now estimates that no fewer than "one in five children will be solicited while online."[5]

Newer technologies have only made matters worse. P2P networks have become magnets for pedophiles and others who exploit children. The National Center for Missing and Exploited Children (NCMEC) "has observed a consistent growth in child pornography" in recent years, partly because of "the popularity of peer-to-peer networking sites."[6] P2P technology makes it easier for pedophiles to access, distribute, and conceal illicit images and videos.[7] And P2P anonymity leads pedophiles to believe they can indulge their perverse fantasies with impunity.[8] For these reasons, the Chairman of a popular peer-to-peer application recently testified before Congress that "P2P networks are plagued by child pornography."[9]

---

[4] S. REP. NO. 106-141, at 4 (1999).

[5] *Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know About Child Predators: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce***,** 109th Cong. (Apr. 6, 2006) (statement of Chris Swecker, Acting Exec. Assistant Dir., Law Enforcement Services, Fed. Bureau of Investigation).

[6] Press Release, Nat'l Ctr. for Missing and Exploited Children, Reports to National Cybertipline Exceed 475,000 (Apr. 24, 2007), *available at* http://www.missingkids.com/ missingkids/servlet/ NewsEventServlet?LanguageCountry=en_US&PageId=3142 (last visited Feb. 22, 2008).

[7] FED. TRADE COMM'N, PEER-TO-PEER FILE-SHARING TECHNOLOGY: CONSUMER PROTECTION AND COMPETITION ISSUES 84 (Dec. 15, 2004), *available at* http://ftc.gov/bcp/workshops/ filesharing/transcript_041215.pdf (last visited Jan. 21, 2005).

[8] *Protecting Children on the Internet: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 110th Cong. 6 (July 24, 2007) (statement of Ernie Allen, President and CEO, Nat'l Ctr. for Missing and Exploited Children), *available at* http://commerce.senate.gov/public/ _files/TestimonyEAllenSenateCommerce7_24_07.doc (last visited Feb. 25, 2008).

[9] *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 110th Cong. 2 (July 24, 2007) (statement of Mark Gorton, Chairman, Lime Wire LLC), *available at* http://oversight.house.gov/documents/2007072410415 5.pdf (last visited Feb. 25, 2008).

A recent study by the Government Accountability Office (GAO) suggests the magnitude of the problem. In one search of P2P networks using 12 keywords known to be associated with child pornography, GAO identified 1,286 titles and file names of which 543 (about 42 percent) were associated with child pornography images. Of the remaining, 34 percent were classified as adult pornography and 24 percent as non-pornographic.[10] Another report noted that the sixth most popular search term on one P2P network was the word "teen"; the eighth was "preteen."[11]

The problem is not just that pedophiles are using P2P to access illicit photos and videos, alone and in the privacy of their own homes, but rather that pedophiles tend to act on the degenerate desires fueled by these materials. A disturbingly high percentage of those who possess child pornography also sexually abuse children. According to a 2005 NCMEC study funded by the Department of Justice, fully 55 percent of people arrested for possessing child pornography also stand accused of child sexual victimization.[12]

II. ISPs Are Instrumental Partners in the Fight Against Child Predators.

ISPs have played indispensable roles in law enforcement's ongoing efforts to bring these predators to justice. In fact, the only reason authorities learned of some crimes is that they were alerted by network operators. Whether by referring tips from subscribers, actively scanning their networks for illicit content, or inadvertently coming across illegal materials in the course of routine network management, ISPs have proven to be invaluable partners in the fight against

---

[10] U.S. GEN. ACCOUNTING OFFICE, GAO-04-757T, USERS OF PEER-TO-PEER NETWORKS CAN READILY ACCESS CHILD PORNOGRAPHY 1, 2 (May 6, 2004).

[11] MIN. STAFF OF SPECIAL INV. DIV., H. COMM. ON GOV'T REFORM, 107TH CONG., CHILDREN'S ACCESS TO PORNOGRAPHY THROUGH INTERNET FILE-SHARING 5 (Comm. Print 2001).

[12] NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, CHILD-PORNOGRAPHY POSSESSORS ARRESTED IN INTERNET-RELATED CRIMES: FINDINGS FROM THE NATION JUVENILE ONLINE VICTIMIZATION STUDY 16 (2005), *available at* http://www.missingkids.com/en_US/publications/NC144.pdf (last visited Feb. 25, 2008).

child pornography and exploitation. The Commission should ensure that any new rules do not interfere with the ability of ISPs to do their part.[13]

For example, in August 2007, an ISP notified NCMEC's CyberTipline that it had discovered graphic pictures on a popular social networking site – including photos of a prepubescent boy kissing a grown man. Further investigation by law enforcement officers revealed the victim to be a ten-year-old schoolchild from Ohio. When interviewed, the boy confirmed that he had been sexually exploited. The suspect – who was working as a teacher's assistant at the victim's elementary school – is now in custody.

That is not the only occasion on which ISPs have helped stop educators from exploiting their students. Three times between December 2006 and January 2007, an ISP tipped off NCMEC that a user was posting sexually explicit photos and videos of children to an Internet group; it also provided the suspect's email address. Authorities soon discovered the suspect was a middle school teacher in Athens, Georgia. He was arrested and charged with sexual exploitation, and now faces 20 years in jail for each image.

Between May 2006 and February 2007, NCMEC received four separate reports that ISPs had discovered a suspect who was uploading sexually abusive photos of children to the Internet. In addition to the images, the ISPs provided NCMEC with the suspect's email address and an Internet Protocol address. When executing a search warrant, New York State Police officers found that the suspect's computer contained more than 600 images of child pornography; officers also found notebooks in which he had recorded his interest in molesting several females in his community. The suspect pled guilty to possessing child pornography. He was sentenced to a ten year prison term – the maximum available – and ten years of supervised probation.

[13] The following examples are from NCMEC's CyberTipline Success Stories, *available at* http://www.ncmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3519.

Predators do not just use the Internet to view child pornography; they also use it to distribute evidence of their own exploitation of children. In November 2006, an ISP provided a tip that a user had uploaded pornographic images of children to an online photo album. Many of the photos depicted a prepubescent girl being sexually assaulted by an adult male. Thanks to the ISP's information, authorities were able to track the suspect – a 46-year-old man – to Boone County, Kentucky. He was arrested and charged with seven counts of first degree sodomy and one count of first degree sexual abuse, and now faces a maximum sentence of life imprisonment.

It bears emphasis that ISPs have uncovered evidence of child exploitation not just by actively monitoring for it, but by accidentally stumbling across it while performing routine systems checks and network maintenance. Officials were able to take down an international child-pornography ring – involving some 2400 predators in 77 countries – because "a man working for a Vienna-based Internet file-hosting service approached authorities at Austria's interior ministry to say he had noticed child pornography being downloaded during a routine check."[14] The Commission's rules should not in any way dissuade ISPs from undertaking the network management that has spawned so many successful child exploitation investigations.

III. The Commission Should Expressly Recognize the Right of ISPs to Monitor, Filter, and Report Child Pornography and Other Illegal Content.

If the Commission decides to issue rules, it should state explicitly that, in the course of managing their networks, ISPs may monitor for the transmission of child pornography and other illegal content, filter sites containing such content, and report such content to authorities. Three discrete considerations support such a policy.

A. It is already implicit in the *Statement* that ISPs are entitled to exclude illegal content from their networks and to report such content to law enforcement. Indeed, three of the

[14] William J. Kole, *40 Arrested in Austrian Child Porn Sweep*, ASSOC. PRESS, May 11, 2007.

Commission's four guiding principles are based on the assumption that Internet users have no right to access illicit materials. The Commission should make it explicit.

The Commission acknowledges that ISP customers may only "access the *lawful* Internet content of their choice." Because users have no entitlement to receive illegal content, the necessary implication is that ISPs cannot be faulted if they manage their networks in a way that denies access to illegal materials. Likewise, the Commission recognizes that the right of consumers to "run applications and use services of their choice" is not absolute, but is necessarily "*subject to the needs of law enforcement*." The implication is that ISPs may alert authorities to any illegal activities they discover in the course of managing their networks. The Commission also stresses that there is a limit to the types of devices subscribers are entitled to use – only "*legal* devices that do not harm the network." The unifying thread that runs through the *Statement* is that subscribers cannot complain if ISPs filter illicit material.

Even Vuze and Free Press appear to agree that ISPs retain the right to filter illegal content and report it to authorities. The very first page of Vuze's petition for rulemaking asks the Commission to prevent network operators from interfering with "*lawful* Internet applications, content, or technologies." Vuze Pet. at 1 (emphasis added). Free Press likewise stresses that many of the applications at issue facilitate "clearly *legal* activities," such as downloading "*Legal* Video Programming." Free Press Pet. at 17, 20 (emphases added). Petitioners have taken pains to clarify that they are not seeking a license to send illegal content over ISPs' networks. The Commission should be equally clear that no such right exists.

B. The second reason the Commission should formally recognize the ability of ISPs to filter illegal materials is straightforward: Doing so will help reduce the amount of child pornography transmitted over their networks. As discussed above, the volume of child

pornography available on the Internet generally – and P2P networks in particular – is staggering. It only takes a few keystrokes for a curious, let alone determined, Internet user to access troves of salacious pictures and videos. Even P2P operators acknowledge that their products are "plagued" by child pornography.[15] (In effect, law-abiding Internet users are subsidizing – in the form of slower Internet service and higher subscription fees – the crimes of bandwidth-hogging child predators. A not-insubstantial portion of P2P traffic consists of predators exchanging massive image and video files. The resulting bandwidth scarcity means ISPs must either increase network capacity, live with slower speeds, or both. Those harms are likely to be passed on to ordinary subscribers. This is the equivalent of law-abiding motorists being asked to pay a gasoline surcharge to finance the construction of special highway lanes for reckless drivers.)

The benefits of curtailing child pornography are too obvious to require extended discussion, but two aspects of the problem deserve special attention. Permitting ISPs to filter illegal materials will help prevent the victims of child pornography from being further victimized by further distribution. Children quite obviously are harmed by the production of pornographic images and videos. But as the Supreme Court has recognized, "the materials are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation."[16] Each time a new predator clicks on a link and downloads a lurid movie, the exploited child becomes a victim all over again.

Allowing ISPs to filter illicit sites also will help prevent Internet users – especially children – from inadvertently encountering child pornography when searching for other content.

---

[15] *See supra* note 7 and accompanying text.

[16] New York v. Ferber, 458 U.S. 747, 759 (1982); *see also id*. at 759 n.10 ("'Because the child's actions are reduced to a recording, the pornography may haunt him in future years, long after the original misdeed took place.'" (quoting Shouvlin, *Preventing the Sexual Exploitation of Children: A Model Act*, 17 WAKE FOREST L. REV. 535, 545 (1981))).

A 2005 GAO report warned that "juveniles continue to be at risk of inadvertent exposure to pornographic images when using P2P programs."[17] All three of the most popular P2P programs returned pornographic images when investigators searched for files "using three innocuous terms likely to be used by juveniles (a popular teenage singer/actress, a popular cartoon, and a popular movie character)"; searches of one P2P network using an "innocuous" word yielded 13 images, 46 percent of which were cartoon pornography.[18]

C. Third, it is vital that the Commission preserve the current ability of ISPs to assist law enforcement officials in investigating crimes involving child pornography and exploitation. In case after case, network operators have tipped off authorities to information that has proven critical in identifying child predators and putting them in jail. It is no exaggeration to say that some unknown number of predators would still be preying on children if it were not for the help of ISPs.

Indeed, ISPs often will be better positioned than other potential gatekeepers to alert authorities to the existence of child pornography and other illegal materials. In the course of monitoring the performance of their networks, ISPs inevitably – if inadvertently – will spot the telltale signs that a particular subscriber is uploading or downloading exploitative content. By contrast, P2P networks *by design* remain ignorant of their users' habits.[19] And a portal web site – such as Google or Yahoo! – may not always know the identity of the user who is employing their search engine to look for child pornography. Indeed, the portal may not know anything at

---

[17] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-634, THE USE OF PEER-TO-PEER NETWORKS TO ACCESS PORNOGRAPHY 3 (May 2005).

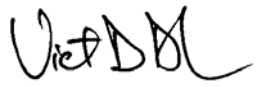
[18] *Id*. at 16, 21.

[19] *See, e.g.*, MGM Studios Inc. v. Grokster, 545 U.S. 913, 922 (2005) ("Grokster and StreamCast use no servers to intercept the content of the search requests or to mediate the file transfers conducted by users of the software . . . ."); *see also id.* at 920 n.1 (emphasizing that, on P2P networks, "it is more difficult to control the content of files available for retrieval and the behavior of users").

all if the user bypasses it altogether and conducts searches through an anonymous P2P network. It may well be true in a given case that if an ISP does not uncover evidence of exploitation, the crime might go undetected and unpunished. Acknowledging that ISPs are justified in reporting illegal content on their networks thus makes sense from an efficiency standpoint.

Importantly, it does not appear that ISPs uncover this evidence of child exploitation primarily because they actively scan their networks for it. In a substantial percentage of cases, they come across it by accident – for example, while conducting routine maintenance of their networks or when performing basic system tests. The ability of ISPs to find evidence of child exploitation and refer it to law enforcement thus is directly related to the robustness of the steps they take to manage their networks. Any laxity in network management inevitably would come at the cost of fewer detections of exploitation and fewer referrals to authorities. For that reason, the Commission should not be content simply to state that ISPs are entitled to actively monitor network traffic for evidence of illegal activity. The Commission also should take pains to ensure that any rules it issues do not hamper ISPs in performing the routine network maintenance that has proven such an obstacle to child predators in the past.

Respectfully submitted,



Viet D. Dinh
Nathan A. Sales
BANCROFT ASSOCIATES PLLC
1919 M Street, NW
Suite 470
Washington, D.C. 20036
Tel: (202) 234-0090

Counsel for the Coalition

February 28, 2008

Certificate of Service

Pursuant to Section 1.47 of the Commission's rules, the undersigned counsel hereby certifies that on this 28th day of February, 2008, a true copy of the foregoing Reply Comments was sent by first class mail to Counsel for Free Press, *et al*.

Viet D. Dinh