



November 16, 2009

Peer-to-Peer File Sharing: Pandora's Box of Child Porn?

Stacie Rumenap

Peer-to-Peer (P2P) networks are a distributed network composed of participants that directly share resources such as processing power, disk storage, and network bandwidth available directly to their peers without intermediary network hosts or servers.¹ P2P networks are intended to remain unaware of their users' habits, creating fertile ground for illicit use such as swapping pornographic material of minors. In some instances files are shared inadvertently. Some frightening examples include sensitive Secret Service memos and IRS tax returns. Federal government employees or contractors who installed P2P software without paying attention to which documents were viewed on the network inadvertently allowed access to

sensitive documents.² New technologies often allow criminals to outpace law enforcement and P2P networks follow this trend, allowing handlers of child pornography to act anonymous and unafraid of prosecution.

The U.S. House of Representatives Committee on Oversight and Government Reform stated that P2P file sharing technology holds "significant risks to American consumers and even to government agencies."³ The U.S. Department of Homeland Security warns that file-sharing technology should be avoided because it "exposes users' computers to infection, attack

¹ Rüdiger Schollmeier, *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).

² Declan McCullagh, "Congress: File Sharing Leaks Sensitive Government Data," CBSNews.com, July 29, 2009

³ U.S. House of Representatives Committee On Oversight And Government Reform Letter to FTC Chairman Jon Leibowitz, April 20, 2009, <http://oversight.house.gov/documents/20090421184216.pdf>

or exposure of personal information.”⁴ Parents are often unaware of the dangers that lurk for their children when searching for music, files or photos of cartoon characters. Children are often inundated with illegal pornographic material when searching for images, music, and video of their favorite singers and entertainers.⁵ Unknown and untracked, a predator can access your child’s files or post explicit images. The decentralized technology creates tracking challenges. Unlike a server, there is no main hub of information and monitoring millions of unique computer connections is difficult.

P2P technology joined the national conversation with the popularity and controversy surrounding Napster and other free music sharing services in the late 1990s. The technology has been in practice much longer, however, with many useful and legal purposes. P2P file sharing accounts for between 43 to 70 percent of Internet traffic, depending on region and quality of the

Internet connection.⁶ Pedophiles turned to P2P file sharers in an effort to avoid law enforcement scrutiny of Internet Service Provider’s (ISP) servers and other aspects of the Internet often policed.

Popular services like Skype use P2P along with other Voice Over IP (VoIP) providers. VoIP accounts for one percent of the Internet traffic but is used by 30 percent of all users.⁷

Drug researchers are also harnessing the power of file sharing to collaborate across oceans for the benefit of patients. In the UK, The Centre for Computational Drug Discovery at the University of Oxford is working with the United States’ National Foundation for Cancer to create what amounts to the world’s second largest supercomputer by pooling their resources. They are using the technology to research new ways to fight pancreatic cancer on a mammoth scale.⁸ Individually the task would have been difficult, but by pooling resources the institutions were able to maximize the research and collaborate.

The Pennsylvania State University began collaborating in 2003 with other

⁴ Brian Krebs and Ellen Nakashima, “File Sharing Leaks Sensitive Federal Data, Lawmakers Are Told,” The Washington Post, July 30, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/07/29/AR2009072902273.html>

⁵ “Children’s Exposure To Pornography On Peer-To-Peer Networks,” U.S. House of Representatives Committee On Oversight And Government Reform, March 2003, <http://oversight.house.gov/documents/20040817153704-85383.pdf>

⁶ Ipoque Internet Study 2007, <http://www.ipoque.com/>

⁷ Ibid.

⁸ University of Oxford, <http://www.chem.ox.ac.uk/cancer/pancreaticcancer.html>

educational institutions across the globe to bring a P2P system to bear to facilitate the global exchange of ideas and research. Partners include the Massachusetts Institute of Technology, Simon Fraser University in Canada and Internet2.

After September 11, 2001, the U.S. Department of Defense began to look for new methods of sharing information, including P2P methods of communicating directly on the battlefield.⁹ The use of P2P technology is being considered for sharing of sensitive military information quickly and directly.

The technology in question has more problems than solutions. Stop Child Predators applauds the efforts of policy makers to safeguard our children, including the 2009 bi-partisan legislation introduced to prevent the proliferation of child pornography by requiring (P2P) file-sharing distributors to obtain informed consent of users before information on their computers is shared. The Informed P2P User Act of 2009 (H.R. 1319) is similar to last year's HR 7176, introduced by Representatives John Barrow (D-GA) and Mary Bono Mack (R-CA). Congress has taken notice of the proliferation of child pornography on P2P, advancing legislation and regulation to contain it.

⁹Walker, Leslie, "Uncle Sam Wants Napster!" The Washington Post, November 8, 2001

Stop Child Predators brings together an influential team of policy experts and community leaders with real-world experience and a track record of proven results to protect children online. Numerous organizations and individuals across the country are motivated by the shared goal of protecting children and holding their victimizers accountable. Stop Child Predators seeks to highlight the dangers of P2P.

P2P and Child Porn

P2P technologies are frequently used for illegal activities. The decentralized and unmonitored approach allows for the sharing of child pornography. In 2006, U.S. Attorney General Alberto Gonzales announced charges against 27 people in the United States, Canada, Australia and Great Britain in connection with an Internet chat room used to trade child porn and view real-time child molestation globally.¹⁰

Federal and local authorities in California arrested seven men on charges of possessing child pornography in an investigation that ultimately led to charges against a total of 52 defendants for allegedly using P2P networks to exchange graphic

¹⁰MSNBC, "27 Charged In Child Porn Bust," March. 15, 2006

images and videos in 2008.¹¹ Arrests included a man featured on *America's Most Wanted* who was living above a child daycare facility in Hollywood while being sought in a child pornography case out of North Dakota.¹²

In September 2009, authorities arrested a Hawaiian man with images of child pornography on his computer that were obtained from a P2P network. Daniel Guerrero produced videos of his own molestation of children. The arrest was linked to an investigation of the same file-sharing network in Oklahoma on which, officials discovered images produced by Guerrero. Video and still images were produced of Guerrero sexually assaulting young children, including a prepubescent boy and a girl in diapers.¹³

MediaDefender, a company with extensive expertise with P2P networks, researched the prevalence of pornography available to children on P2P networks on behalf of the U.S. House of Representatives Committee on Oversight and Government Reform in 2003. The discoveries were shocking. Approximately six million pornographic files were available for downloading on one popular P2P network

over a two-day period.¹⁴ The U.S. Government Accountability Office also investigated the prevalence of pornography on P2P. A sample of 341 images was captured and over 50% were pornographic images of children.¹⁵

The Federal Trade Commission (FTC) reported that P2P technology makes it easier for pedophiles to access, distribute and conceal illicit images and videos, putting consumers at risk. Consumers, including children, may inadvertently expose themselves to pornographic or other illicit materials. Consumers may also distribute files containing child pornography exposing themselves to potential criminal liability.¹⁶

The problem is as widespread as it is dire. In the decade since the Federal Bureau of Investigations (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

¹¹ FBI, Los Angeles Field Office Press Release, August 19, 2008, <http://losangeles.fbi.gov>

¹² Ibid.

¹³ Honolulu Star-Bulletin, "Convicted Thief Accused Of Producing Child Porn," September 11, 2009

¹⁴ "Children's Exposure To Pornography On Peer-To-Peer Networks," U.S. House of Representatives Committee On Oversight And Government Reform, March 2003, <http://oversight.house.gov/documents/20040817153704-85383.pdf>

¹⁵ "Children's Exposure To Pornography On Peer-To-Peer Networks," U.S. House of Representatives Committee On Oversight And Government Reform, March 2003, <http://oversight.house.gov/documents/20040817153704-85383.pdf>

¹⁶ FTC, "Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues," 2005, <http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>

“one in five children will be solicited while online.”¹⁷

In February 2008, Stop Child Predators joined the Christian Coalition of America, The CP80 Foundation and Enough Is Enough in submitting reply comments to the Federal Communications Commission (FCC) reply comments of *Free Press, et al.*¹⁸ The coalition was concerned that approval of the Vuze and Free Press petitions might make it more difficult for ISPs to monitor and filter the use of anonymous and decentralized P2P networks to “facilitate crimes against children, and to report those crimes to authorities.”

The coalition called on the FCC to expressly require ISPs to actively search their networks for illicit materials and acknowledge the reality of how computer crimes are actually uncovered. Sometimes ISPs discover evidence of criminal activity because they are looking for it. However, sometimes they come across it in the course of routine network management. The coalition called on the Commission to 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.¹⁹

In June 2007, Stop Child Predators also joined child advocacy organizations in weighing in on *United States v. Michael Williams* before the U.S. Supreme Court. Along with the Jessica Marie Lunsford Foundation, The Joyful Child Foundation, The KlaasKids Foundation and the National Law Center for Children and Families, Stop Child Predators argued that the Court of Appeals wrongly invalidated an effective and constitutional tool for ceasing the marketing and trafficking of child pornography over the Internet. By criminalizing advertising and promoting child pornography (as opposed to the actual possession or distribution itself), the coalition argued that the PROTECT Act’s “pandering” provision properly allows the government to prosecute a would-be purveyor or consumer of child pornography.²⁰

¹⁷ “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 Congress, April 6, 2006

¹⁸ Stop Child Predators joined Christian Coalition of America, The CP80 Foundation and Enough Is Enough in reply comments to the FCC reply comments of Free Press, et al., http://www.stopchildpredators.org/pdf/Coalition_Co_mments.pdf

¹⁹ Stop Child Predators joined Christian Coalition Of America, The CP80 Foundation and Enough Is Enough in reply comments to the FCC reply comments of Free Press, et al., http://www.stopchildpredators.org/pdf/Coalition_Co_mments.pdf

²⁰ Stop Child Predators, Friend of the Court Brief, US v Michael Williams, http://www.stopchildpredators.org/pdf/Williams_Am_icus_Brief.pdf

Who is Safeguarding Our Children?

Parents are the first line of defense; we must take responsibility for the safety of our children. Many parents set up filtering software on their computers and sit back. The FTC cautioned that this approach had “substantial limitations in excluding pornography.”²¹ Many filtering tools do not include the capability to monitor P2P activity.

Federal and local law enforcement organizations generally take the lead in investigation and prosecution of crimes committed using P2P networks. Recent estimates tallied more than 1,000 investigations in the United States involving the distribution and possession of child pornography over these networks.²²

Pornographers are using new techniques and elaborate masking technologies to continue their practice. Law enforcement is close behind, recently discovering the use of a practice of infiltrating a computer without a user’s knowledge with a “bot” or a “zombie.” A U.S. Department of Justice official highlighted P2P as a top concern when addressing new Internet

technologies used to assist child porn.²³ The FBI, U.S. Department of Homeland Security and U.S. Immigration and Customs play a regular role in tracking offenders and bringing them to justice.

P2P providers created an extensive public relations campaign to portray the industry as a partner with law enforcement, eager to do their part in an effort to highlight child pornographers when possible. The industry’s trade association launched a campaign in 2004 to educate consumers but with little real action since inception. The Association praises the enforcement actions of the FBI, who they claim to “have worked cooperatively since October 2003.”²⁴

Sharman Networks, owner of music sharing site Kazaa, sent executive Alan Morris to address the U.S. Senate Judiciary Committee in 2003 declaring “we totally abhor child pornography.”²⁵ Mr. Morris also admitted the company cannot control what is distributed on their network, calling it

²¹ “Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues,” Federal Trade Commission, June 2005,

<http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>

²² Jay Lyman, TechNewsWorld, “Feds Crack Down on P2P Child Porn,” May 17, 2004, <http://www.technewsworld.com/story/33836.html?wlc=1253126808&wlc=1253726085>

²³ Ibid.

²⁴ John Borland, Net, “P2P Group Launches Site To Combat Child Porn,” December 12, 2004, http://news.cnet.com/P2P%20group%20launches%20site%20to%20combat%20child%20porn/2100-1025_3-5488290.html

²⁵ “The Dark Side Of A Bright Idea: Could Personal And National Security Risks Compromise The Potential Of Peer-To-Peer File-Sharing Networks?” Hearing Before The Committee On The Judiciary United States Senate One Hundred Eighth Congress, June 17, 2003. <http://www.gpo.gov/congress/senate/pdf/108hr91213.pdf>

“physically impossible.”²⁶ He did, however, highlight the company’s use of filters, password protection and classifications of material to safeguard children as much as possible. Mr. Morris highlighted the company’s advocacy of education and parent supervision for all children using the Sharman Networks’ products.

Thomas Spota, district attorney for Suffolk County, New York, filed child pornography charges in 2003 against 12 Kazaa users. Mr. Spota called for federal legislation “to combat this scourge” of child pornography. He believes that “we need a federal task force...in order to be able to attack the owners and the distributors of these programs, who are reaping enormous profits.”²⁷

Mark Gorton, chairman of Lime Wire LLC, told members of Congress that “P2P networks are plagued by child pornography.”²⁸ The problem persists, but the industry claims to be creating safeguards. Mr. Gorton called upon Congress to create an effective policy and more regulations.

²⁶ Ibid.

²⁷ Grant Gross, “Peer-to-Peer Child Porn Targeted,” PC World, September 9, 2003

²⁸ Testimony of Mark Gorton Chairman, Lime Wire LLC before the Committee on Oversight and Government Reform U.S. House of Representatives, July 24, 2007, <http://oversight.house.gov/documents/20070724104155.pdf>

The National Center for Missing & Exploited Children is an influential advocate for children and families. Robbie Callaway, chairman of the board of directors, drew concern that the use of “file-sharing programs to trade, distribute and disseminate child pornography is significant and growing dramatically.”²⁹ Ernie Allen, president & CEO, said that “many distributors of child pornography are using peer-to-peer file-sharing networks.” Networks without a centralized cache of information are hard for law enforcement to track, and easy to remain anonymous for purveyors of child pornography. Mr. Allen highlighted the organization’s experience with investigations of tips, telling members of Congress that it is “almost impossible to identify the perpetrators responsible for trading the illegal files” over P2P networks.³⁰

John Netherland, former director of the U.S. Department of Homeland Security’s Cyber Smuggling Center, said P2P networks are coming under increased scrutiny.

²⁹ “National Center For Missing & Exploited Children Says File-Sharing Programs Being Used To Distribute Child Pornography,” Press Release, September 8, 2003

³⁰ Ernie Allen, The National Center For Missing & Exploited Children, U.S. Senate Committee On Commerce, Science And Transportation, “Protecting Children on the Internet,” July 24, 2007, http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Testimony&Hearing_ID=008f7aad-96d2-40ed-b375-fe8c254fc213&Witness_ID=e38c4d81-76be-43cb-b7da-62363eb09130

Evidence is increasingly easier to capture and preserve on a real-time basis. “For these reasons peer-to-peer file-sharing investigations are likely to increase.”³¹

Federal lawmakers expect technological improvements in the future, including the use of promising new software designed to detect child pornography called “Operation Fairplay.”³² Special Agent Flint Waters, lead agent for the Wyoming Internet Crimes Against Children Task Force, describes the system as a “comprehensive computer infrastructure that gives law enforcement the tools they need to leverage the latest technologies to identify and track those who prey on children, just as the offenders use technology to identify and track the children that would be their prey.”³³

Congressional Involvement in P2P Protection

Bi-partisan legislation is currently being debated in the U.S. House of Representatives. Representatives John Barrow (D-GA) and Mary Bono Mack (R-CA)

³¹ Declan McCullagh, “Congress mulls new P2P porn restrictions,” CNET, March 13, 2003

³² Anne Broache, “Senators OK \$1 billion for online child porn fight,” CNet, May 16, 2008

³³ Testimony of Special Agent Flint Waters, Lead Agent for the Wyoming Internet Crimes Against Children Task Force, United States Senate Committee On The Judiciary Subcommittee On Crime And Drugs, “Challenges and Solutions for Protecting our Children from Violence and Exploitation in the 21st Century,” April 16, 2008

introduced the Informed P2P User Act of 2009 (H.R. 1319) to prevent the proliferation of child pornography by requiring P2P file-sharing distributors to obtain informed consent of users before information on their computers is shared. Similar legislation was introduced in 2008 by Representatives John Barrow (D-GA), Mary Bono Mack (R-CA) and Joe Barton (R-TX).

During a July 2009 U.S. House Oversight and Government Reform Committee hearing, Chairman Edolphus Towns (D-NY) stated his intentions of creating his own legislation after hearing of the pervasive distribution of child pornography over P2P networks. Chairman Towns was especially chilled to discover the availability of sensitive government documents such as the First Lady’s private itinerary, Secret Service documents and other official records. Chairman Towns is crafting his legislation around limitations of P2P software on “all computer networks operated by the federal government or its contractors.”³⁴ Representative Peter Welch (D-VT) shares Chairman Towns’ concern, and inquired during a July 2009 hearing about potential legal actions that could be taken to protect children from pornography.³⁵

³⁴ Declan McCullagh, “Congress: File Sharing Leaks Sensitive Government Data,” CBSNews.com, July 29, 2009

³⁵ Ibid.

Vice President Joe Biden sponsored the Combating Child Exploitation Act while a senator in 2008. The bill, which became law in October 2008, allocated over \$1 billion over the next eight years to promote increased enforcement of Internet crimes against children. A provision requires 250 new federal agents dedicated to child exploitation cases for beefing up personnel, equipment and educational programs designed to combat Internet crimes against children, and for creating new forensics laboratories if the Attorney General deems it necessary to deal with a 'backlog' of online child exploitation cases.³⁶

Conclusion

Chris Swecker, acting executive assistant director of law enforcement services for the FBI, called child pornography a problem both widespread and dire. In 1996, the FBI launched an initiative to combat child pornography. In 1996, the number of such cases jumped by 2,050 percent, from 113 to 2,500 in only a decade. The FBI now estimates that no fewer than "one in five children will be solicited while online."³⁷

³⁶ Anne Broache, "Senators OK \$1 billion for online child porn fight," CNet, May 16, 2008

³⁷ "Sexual Exploitation of Children Over the Internet: What Parents, Kids and Congress Need to Know About Child Predators," Hearing Before the House of Representatives Subcomm. on Oversight and

Protections are trying to keep pace with technology but the problem continues. In October 2009, the U.S. House of Representatives Energy & Commerce Committee passed the Informed P2P User Act. The legislation is moving to the House floor as this report is compiled, requiring P2P software vendors to supply "clear and conspicuous" notice of which files are shared and obtain consent by computer users before sharing commences. The legislation also prohibits P2P programs from being "sneaky," "surreptitious" and from preventing software that cannot be removed.³⁸

Ernie Allen, president and CEO of the National Center for Missing & Exploited Children, stated it well: "As technology evolves, so does the creativity of the predator. New innovations such as webcams and social networking sites are increasing the vulnerability of our children when they use the Internet. New technology to access the Internet is used by those who profit from the predominantly online market in child pornography and seek to evade detection by law enforcement."³⁹ Law enforcement,

Investigations of the H. Comm. on Energy and Commerce, April 6, 2006

³⁸ Nate Anderson, "Informed P2P User Act To Clamp Down On Filesharing Software," Ars Technica, October 1, 2009

³⁹ President and Chief Executive Officer National Center for Missing & Exploited Children, "Protecting Children on the Internet, July 24, 2007, <http://commerce.senate.gov/public/index.cfm?FuseA>

legislation and regulation must keep pace with technological advances in order to protect our children from the dangers from P2P networks. The FTC recommends industry and government take steps so that consumers receive the many benefits from this technology while avoiding the risks that it creates.⁴⁰ Our nation's children need regulations to ensure P2P networks and other technologies do not put their security at risk.

**Published by Stop Child Predators
1419 37th Street, NW, #108
Washington, DC 20007
(202) 248-7052
www.stopchildpredators.org**

ction=Hearings.Testimony&Hearing_ID=008f7aad-96d2-40ed-b375-fe8c254fc213&Witness_ID=e38c4d81-76be-43cb-b7da-62363eb09130

⁴⁰Federal Trade Commission, June 23, 2005,
<http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>

Additional Resources

- “The Dark Side Of A Bright Idea: Could Personal And National Security Risks Compromise The Potential Of Peer-To-Peer File-Sharing Networks?” Hearing Before The Committee On The Judiciary United States Senate One Hundred Eighth Congress, June 17, 2003, <http://www.gpo.gov/congress/senate/pdf/108hr/91213.pdf>
- “Children’s’ Exposure To Pornography On Peer-To-Peer Networks,” U.S. House of Representatives Committee On Oversight And Government Reform, March 2003, <http://oversight.house.gov/documents/20040817153704-85383.pdf>
- “File-Sharing Programs: Child Pornography Is Readily Accessible Over Peer-to-Peer Networks,” General Accounting Office, February 2003, <http://oversight.house.gov/documents/20040817153544-53182.pdf>
- “Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues,” Federal Trade Commission, June 2005, <http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>
- “Stop Child Predators Supports Legislation Restricting Access to Child Pornography, Urges Congress to Pass Informed P2P User Act,” Press Release, March 04, 2009, <http://www.stopchildpredators.org/news/pr030409.htm>
- “Stop Child Predators Supports Legislation Restricting Access To Child Pornography,” Press Release, September 27, 2008, http://www.stopchildpredators.org/pdf/SCP_Supports_Legislation_092708.pdf