Volume 6, Number 1, 2012

UPDATE

Unsafe Havens II: Prosecuting Technology-Facilitated Crimes Against Children March 5 – 9, 2012

Held at AOL in Sterling, Virginia This is an advanced trial advocacy courts focusing on the prosecution of technology facilitated child sexual exploitation cases. In addition to presentations on related topics, students will conduct a trial from opening statements to presenting the state's case to cross-examining a defense expert to closing statements.

Please contact NCPCA Senior Attorney Justin Fitzsimmons at jfitzsimmons@ndaa.org or (703) 519-1695 for additional information about these courses.

Continued on page 5

Update is a newsletter published by NDAA's National Center for Prosecution of Child Abuse. To change your mailing address for this publication only, send changes, additions and deletions to mhernandez@ndaa.org. Please mention that you are making changes to the *Update* newsletter.

Peer-to-Peer File Sharing Networks and Child Pornography: Possession or Dissemination? Charging Decisions and Other Issues

Part II of II

By Justin T. Fitzsimmons, J.D.[1]

This Update is part two of a two part series. Part one covered what is a peer-to-peer network as well as how one works. Part two of this series covers the different ways a prosecutor may charge child pornography cases arising from a peer-to-peer network and discusses computer forensic artifacts that may be useful in determining appropriate charges.

When prosecutors are faced with the difficult decision of whether to charge possession or dissemination for child pornography in the context of file sharing networks, prosecutors must first ask the question whether the act of file sharing meets the elements of dissemination. The short answer: most likely. Based on current case law and the manner in which the peer-to-peer networks are set up, generally, the prosecution of a defendant using a peer-to-peer file sharing network to obtain child pornography constitutes dissemination or distribution. A thoughtful prosecutor must carefully analyze all of the available evidence, including the results of the computer forensic examination as well as applicable case law before deciding to charge a defendant with more serious crimes. This article will discuss cases evaluating the application of dissemination charges when a defendant uses a peer-to-peer client. Additionally, it will provide the reader with a checklist of the computer forensic artifacts a prosecutor should understand before filing counts of dissemination or distribution of child pornography. Finally, it will discuss the issue of whether a suspect has a right to privacy in his peer-to-peer files once he has downloaded the underlying software.

One of the seminal, oft-cited cases involving whether a peer-to-peer network constitutes distribution or dissemination of child pornography is *United States v. Shaffer*, 472 F.3d 1219 (10th Cir. 2007). In *Shaffer*, an agent of Immigrations and Customs Enforcement from the Department of Homeland Security noticed that a user of the Kazaa peer-to-

peer network with a screen name of shaf@kazza was sharing what he believed were multiple images and movies of child pornography.[2] The agent downloaded files from the screen name shaf@kazza. The investigation revealed that the defendant was a 27-year-old student from Kansas. Based on the preliminary work of the initial agent a subsequent agent secured a search warrant for the defendant's home and computer.[3] During the subsequent computer forensic examination agents recovered 19 images and 25 movie files containing child sexual exploitation.[4] Additionally, the search revealed evidence of documents containing stories of adults having sexual relationships with children.[5]

Following his conviction for distribution of child pornography, the defendant appealed, arguing that he could not be convicted of distribution, but only the lesser charge of possession. The defendant argued that his conduct of downloading images from a peer-to-peer network and storing them in his shared folder only met the elements of possession.[6] The Tenth Circuit Court of Appeals disagreed maintaining the defendant's conviction by holding:

> "We have little difficulty in concluding that Mr. Schaffer distributed child pornography in the sense of having 'delivered,' 'transferred,' 'dispersed,' or 'dispensed' it to others. He may not have actively pushed pornography on Kazaa users, but he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those images. It is something akin to the owner of a self-serve gas station. The owner may not be present at the station, and there may be no attendant present at all. And neither the owner nor his agents may ever pump gas. But the owner has a roadside sign letting all passersby know that, if they choose, they can stop and fill their cars for themselves, paying at the pump by credit card. Just because the operation is self-serve, or in Mr. Shaffer's parlance, passive, we do not doubt for a moment that the gas station owner is in the business of 'distributing,' 'delivering,' 'transferring,' or 'dispersing' gasoline; the raison d'être of owning a gas station is to do just that. So, too, a reasonable jury could find that Mr. Shaffer welcomed people to his computer and was quite happy to let them take child pornography from it."[7]

Expanding on the Tenth Circuit's analogy of a self-serve gas station the Eighth Circuit Court of Appeals, in *United States v. Sewell*, reasoned, "No one would stop at the station without the sign telling them where the gas station is; the context of such a sign tells motorists that the owner of the station is offering to distribute fuel."[8] The *Sewell* court commented on how the process of indexing of files on peer-to-peer file sharing networks acts as a directory of available files, notifying other users of the network what files are contained in a particular user's shared folder. In *Sewell*, the court upheld the conviction for publishing a notice that offered distribution of child pornography through the Kazaa peer-to-peer file sharing program.[9]

Other courts have also focused on the defendant's knowledge of the operation of the peer-to-peer networks to determine criminal culpability. The Texas Court of Appeals in *Wenger v. State*, preserved a conviction for promotion of child pornography, based on dissemination through a peer-to-peer network.[10] In the ruling, the *Wenger* Court found the evidence was sufficient to show the defendant's knowledge even though he claimed he did not understand "how to not share and share and separate those items out."[11] The defendant admitted that he was aware that the peer-to-peer software shared his files and that other users of the software downloaded files from him. Additionally, the court focused on testimony, most likely from the forensic examiner, that the defendant changed the default setting of the program to not automatically share his files which demonstrated his knowledge of how to share and not share files.[12]

Similarly, the Fifth Circuit considered whether the underlying purpose of the peer-to-peer software application, file sharing, justified the imposition of trafficking in child pornography as a sentencing enhancement under the federal sentencing guidelines.[13] The court reasoned that use of the Limewire system allowed a user to share or barter files and that such action fell

within the definition of trafficking of child pornography.[14] The court not only ruled that the defendant's conduct using Limewire constituted distribution, but the defendant was aware of it as he was warned at least two different times during the installation program.[15]

In *United States v Darway*, the Sixth Circuit reviewed and rejected the defendant's contention that use of peer-to-peer software failed to meet the definition of distribution under the federal sentencing guidelines.[16] The defendant unsuccessfully argued that his action was passive and in order to rise to the level of distribution he would have had to actively send images to others over the network.[17]

Likewise the Seventh Circuit in *United States v. Carani* ruled that utilizing a peer-to-peer network qualified as dissemination under the federal sentencing guidelines.[18] In an effort to overcome the defendant's claim of lack of knowledge of how the file sharing software program worked, the prosecution presented testimony of the computer forensic examiner, Agent Skinner from the Department of Homeland Security's Immigration and Customs Enforcement Cyber Crimes Center. Agent Skinner testified about the variety of terms associated with child pornography and the frequency of those terms being used by someone with access to the defendant's computer.[19] The *Carani* Court also pointed out agent Skinner's testimony related to the defendant's elevated participation level on Kazaa.[20]

Following the same logic the Court of Appeals for the Ninth District in Ohio, in *State v. Butler*, upheld a conviction for pandering in child pornography based on the usage of a peer-to-peer file-sharing network.[21] The defendant unsuccessfully argued that the state failed to demonstrate he had knowledge of the six specific files containing child pornography.[22]

As the courts in both *Carani*[23] and *Butler*[24] demonstrate, the underlying forensic examination and interview of the defendant are crucial to elevate peer-to-peer cases from simple possession to dissemination or distribution.[25] To raise a case from simple possession to distribution courts rely on testimony regarding the forensic artifacts[26] to determine a defendant's knowledge of how the underlying peer-to-peer system enables files to be shared with other users.[27]

Another rejected defense is the partial download. Most of the peer-to-peer file sharing networks are set up to allow for portions of a file to be downloaded from multiple sources within the network. This allows for faster downloads across the network. For example, a computer that either has a particular file that may become overloaded with requests or that has a slow Internet connection will delay the entire download process. To speed up the process the networks are arranged to allow the computer to request the missing portions of the file from different computers attached to the network that also have the exact same file. Defendants have claimed that contributing to this partial download does not create a completed child pornography image or movie. In *United States v. Schade*, the Court of Appeals for the Third Circuit considered and rejected this argument, ruling that, at the very least, a defendant who downloads and utilizes a peer-to-peer file sharing network aids and abets in making child pornography available.[29]

The Colorado appellate courts have determined that the use of a peer-to-peer file sharing program does not equate to preparing material under the felony sexual exploitation of a child statute. In *People v. Mantos*, a defendant was charged in a two-count felony indictment with preparing sexually exploitive material and possessing with the intent to distribute sexually exploitive material.[30] The defendant was found not guilty of the possession with intent to distribute count, but guilty of count one, that he "prepared" the child pornography.[31] The defendant appealed the conviction arguing that he did not "prepare" sexually exploitive material.[32] The appellate court considered the question of whether the use of the computer file sharing software Kazaa Light fit within the statutory definition of "prepares" or "arranges for" under the exploitation statute.[33] Conducting its statutory interpretation, the *Mantos* Court looked at the common meaning of the word "prepare" and, citing Webster's Third New International Dictionary 1790-91, (2002) determined that the proper meaning of prepare was to "make, or produce."[34] The court took the rationale one step further, concluding that producing also includes a creative process that results in a finished product, for example

cooking a meal or developing a speech.[35] In dicta, the court noted that the legislature did not intend that the use of file sharing software for the type of conduct defendant engaged in go unpunished, but rather the jury found the defendant not guilty of that conduct.[36]

In *United States v. Handy*, the District Court from the Middle District of Florida acknowledged the rationale underlying the decisions the Eighth and Tenth Circuits holdings in *Sewell and Schaefer*, determining that a person utilizing peer-to-peer client software can be convicted of distributing child pornography.[37] However, the court ultimately determined that the prosecution failed to provide any evidence that the software was configured to allow the sharing of files.[38] In *Handy*, the court reviewed the different types of peer-to-peer file sharing software packages and determined that without additional evidence presented by the government an enhancement for distribution should not be added.[39] The *Handy* Court cautioned other courts making similar determinations to conduct a thorough review relating to the specific mechanisms of the peer-to-peer application used by the defendant.[40]

Another failed defense is the claim that a defendant has a privacy right in files placed in his shared file folder. Underlying the premise of this argument is the flawed perception that law enforcement engages in a search of the suspect's computer when looking for images and movies on peer-to-peer networks.[41] Courts have routinely rejected this argument, ruling that defendant in essence, is advertising his shared files to anyone else on the network. Courts have rejected the defense premise that the officers are "searching" inside a defendant's computer through this process.[42] Instead, courts have understood the explanation of the technology supporting the peer-to-peer networks to mean each computer on the network creates an index of the files in its shared folder of that specific peer-to-peer network and advertises the list of those files to every other user of the network.

Conclusion

A prosecutor analyzing an investigation involving the use of a peer-to-peer network should take steps to determine the appropriate charges to file against a defendant. That review must involve comparing the available evidence to the elements for the crimes of distribution and dissemination of child pornography. Initially, a prosecutor should speak with his or her investigator and/or computer forensic examiner to determine whether sufficient evidence of the defendant's knowledge of how a peer-to-peer file sharing network works exists. The computer forensic examination should be reviewed for specific key words and data demonstrating intent to access child pornography.[43] A prosecutor should review the defendant's statement to determine what evidence of that knowledge is present. Hopefully, this includes specific knowledge of the defendant's computer usage, whether the defendant installed the software program, whether the defendant changed any of the default settings, and whether the defendant admitted to understanding that the peer-to-peer network is based on file sharing.[44] If this evidence is present elevated charges may be appropriate.

[1] Senior Attorney, National District Attorneys Association's National Center for Prosecution of Child Abuse.

[2] *United States v. Shaffer*, 472 F.3d 1219, 1222 (10th Cir. 2007).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.* at 1220.

[7] *Id.* at 1223-1224. The Court explained its decision by detailing the user manual of Kazaa, which includes the simple steps necessary for a user to download a file and puts the user on notice that a file in the shared folder is accessible to any other Kazaa user. The court noted that there are only two ways to place a file within the shared folder, either downloading it from a different shared folder or moving it from another place on the computer to the shared folder. In either case the court noted the effort to place a file within the shared folder was a conscious choice of the user. *Id.* at 1222. The court also rejected the defendant's proffered expert's opinion that the defendant was merely on a "porn fishing expedition" instead of seeking out images of child pornography as that testimony would touch on the defendant's state of mind which was a matter for the jury to decide. *Id.* at 1225.

[8] *United States v. Sewell*, 513 F.3d 820 (8th Cir. 2008).

[9] The court described how a user of Kazaa may run a key word search on the network that will generate a list of files that are offered by other users on the network. The list of those files in an offender's shared folder constitutes a notice of an offer sufficient to uphold the criminal charge. *Id.* at 822.

[10] *Wenger v. State*, 292 S.W.3d 191 (Tex. Crim. App. 2009).

[11] *Id.* at 200.

[12] *Id.* at 200-202.

[13] *United States v. Todd*, 100 F.App'x. 248 (5th Cir. 2005), vacated on other grounds, 543 U.S. 1108 (2005).

[14] *Id.*

[15] *Id.* at 250.

[16] *United States v. Darway*, 255 Fed. App'x 68, 70, 207 U.S. App. LEXIS 26422 (6th Cir. 2007).

[17] *Id.* at 70-71.

Unsafe Havens I: Investigation and Prosecution of Technology-Facilitate Child Sexual Exploitation
Date: Summer 2012, Location TBD

This comprehensive five-day course is designed to familiarize prosecutors with the various stages of an investigation, pre-trial and case preparation of a child sexual exploitation case that has been facilitated through technology. This course includes a hands-on computer lab.

SafetyNet: Multidisciplinary Investigation and Prosecution of Technology-Facilitated Child Sexual Exploitation
Date: Early Fall 2012, Location: TBD

This intensive five-day course is intended for prosecutors, investigators and computer forensic examiners, investigation and prosecuting technology-facilitated child sexual exploitation cases. This course includes mock trial exercises and a hands-on computer lab.

This project was supported by Grant No. 2010-MC-CX-K048 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

[18] *United States v. Carani*, 492 F.3d 867, (7th Cir. 2007).

[19] *Id*. at 872. The terms and frequency of use agent skinner testified to were: "pedophilia, young Lolita, kiddie, preteen, kindersex, pedo, BabyJ, Baby J, pedo video, illegal pedophilia, r@ygold, underage, incest, Lolita, kiddie porn, real kiddie, kinder and child lover…(with the frequency for the following terms] 3050 hits for "kiddie," 2,011 hits for "preteen," 3,603 hits for "pedo," 1,799 hits for "r@ygold," and 3,720 hits for "Lolita." *Id*.

[20] *Id*. at 871. The court noted, based on agent Skinner's testimony, that Kazaa download speeds are based on a participation system. The more a user participates in sharing files the faster the user receives downloaded files. The system has a maximum of 1,000. The defendant's level was 771. The court noted how the prosecution presented evidence that this was based on a special hack application that allowed the computer to download from itself, giving the appearance of a greater participation rate on Kazaa network. The Agent testified the setting was not passive and required action by the computer user. *Id*.

[21] *State v. Butler*, 2009 WL 1067051 (Ct App. Ninth Dist. 2009)

[22] *Id*. *But see, People v. Vescoso*, No. 272404, 2007 WL 4404568 at *4, (Mich. Ct. App. 2007) (Unpublished Opinion) (where the court reversed a defendant's conviction for distribution of child sexually abusive material based on an improper jury instruction as to defendant's requisite knowledge of whether the peer-to-peer program shared files to others. In dicta, the court noted there was scant, if any evidence presented of defendant's understanding or knowledge of the inner workings of the network.

[23] *Carani*, 492 F.3d 867.

[24] *Butler,* 2009 WL 1067051.

[25] Or the possible equivalent criminal statute depending upon individual state statutory schemes. See: http://www.ndaa.org/pdf/Child%20Pornography%20Distribution%20Statutes%203-2010.pdf.

[26] By forensic artifact, the author is referring to specific data or files found during the computer forensic examination of a defendant's digital storage device that contain relevant information relating to the underlying charge. These artifacts may include, but are not limited to, Registry settings, program preferences, index.dat files, .lnk files, typed URL's, specific keyword searches associated with child pornography.

[27] *See Supra* note: 16.

[28] When a file is transferred through a peer-to-peer network the file does not travel as a complete file, the data making up the file is broken up into packets of information. Those packets are sent separately over the Internet and then reconfigured once they arrive back at the computer that requested the file. Sometimes, a file does not completely transfer. This is referred to as a partial download, when some, but not all of the packets are received. It is possible to view part of the file in these cases. However, an officer who is relying upon this for a warrant should make sure that he or she includes that information in the affidavit for the warrant.

[29] *United States v. Schade*, 318 Fed.App'x. 91, 94 (3rd Cir. 2009).

[30] *People v. Mantos*, 250 P.3d 586 (Colorado Ct. App. Div I., 2009). Factually, the defendant had the master sharing option of KAZAA Light turned to "not share" but had each individual file within the shared folder available for sharing. *Mantos*, 250 P.3d at 588.

[31] *Id*. at 587. (the charge alleged that the "defendant, in violation of section 18-6-403(3)(b), 'prepared, arranged for, published, produced, promoted, made, sold, financed, offered, exhibited, advertised, dealt in, or distributed any sexually exploitative material.'").

[32] *Id*. at 588.

[33] *Id*. at 590.

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] *United States v. Handy*, No. 6:08-cr-180-Orl-31DAB, 2009 WL 151103, (M.D. Fla. Jan. 21, 2009).

[38] *Id*. at *3.

[39] *Id*. at *2.

[40] *Id*. at *3. The court concluded that a sentencing court should bear in mind the type of application used by a defendant, whether the application has the ability to simultaneously upload files to other users while being downloaded by a defendant; whether the downloaded file was kept in a shared folder; review the evidence to determine whether a defendant limited access to specific files, child pornography, within the shared folder. *Id*.

[41] *See, e.g., United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *see also Ohio v. Thornton*, No. 09AP-108, 2009 WL 3090409, 2009 Ohio 5125 (Ohio. Ct. App. Sept. 29, 2009).

[42] *See e.g., Ganoe*, 538 F.3d at 1127; *Thornton*, 2009 WL 3090409 at *3.

[43] Key word searches have the possibility of providing doubly incriminating evidence. First, the presence of certain key words in the peer-to-peer file sharing application demonstrates the intent to acquire child pornography. Second, if the key words exist outside of the peer-to-peer file sharing network it eliminates the accidental download defense. In order for evidence of a key word, for example, pthc (pre-teen hardcore), to appear outside of the peer-to-peer application the user would have to take additional affirmative steps. There is no automatic process that would move files with such key words to different areas of a digital storage device or hard drive.

[44] This is certainly not an exhaustive list and there are additional questions and forensic artifacts that will demonstrate a defendant's knowledge of the underlying peer-to-peer network.