Peer-to-Peer File Sharing Case Law Review

By Dennis Nicewander
Assistant State Attorney
Broward County, Florida

Overview

This legal outline discusses the existing case law interpreting peer-to-peer file sharing investigations involving child pornography. I have attempted to include all state and federal appellate decisions addressing issues unique to investigative techniques currently used to locate and prosecute individuals trading child pornography on peer-to-peer networks. There are two significant areas of case law related to peer-to-peer file sharing that I have chosen not to cover. The first concerns litigation by the music industry against individuals trading copyrighted music. These cases occasionally address such issues as expectation of privacy in shared folders, but since there are numerous criminal cases discussing the same issue, I have chosen not to include them. I have also chosen not to include the numerous federal decisions that discuss whether using a peer-to-peer program such as LimeWire qualifies for an enhancement under the federal sentencing guidelines. Most cases indicate that the enhancement applies, but the government must show that the defendant had actually configured the software to share files. Simply proving the software is on the computer is not enough.

The case law on the topic is overwhelmingly in favor of the government. The only case that went against the government was U.S. v. Stevahn, where the federal court ruled that the search warrant affidavit did not adequately describe the reliability of the Peer Spectre program. The good faith exception saved the warrant in this case.

The majority of the existing case law concerns unpublished federal decisions discussing whether defendants were entitled to *Franks* hearings based upon false or misleading facts or omissions in the search warrant affidavits. These decisions have ultimately favored the government, but a careful reading of them demonstrates many pitfalls that await the unprepared investigator. These cases typically provide a detailed overview of peer-to-peer investigative techniques and the technical issues involved.

The second most common issue addressed concerns whether a defendant has a reasonable expectation of privacy in his shared folder. The courts have routinely ruled that no such expectation of privacy exists.

The third most common issue addresses whether sharing child pornography in the user's shared folder is sufficient to convict a defendant of distribution. Most of the case law favors the government's efforts to charge distribution in these circumstances.
This outline will be organized by the general issues discussed. The general topics included at this time are as follows:

Franks Hearings:

This hearing got its name from Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). As a preliminary matter, a defendant is only entitled to a *Franks* hearing if he makes a substantial showing that an affiant to a search warrant application knowingly or intentionally, or with reckless disregard for the truth, made false statements or omitted material facts and that the alleged statements were necessary to a finding of probable cause. If the affidavit no longer establishes probable cause after the false or misleading statements are removed, the evidence will be suppressed.

Even though the case law is favorable on this issue, a careful reading of the opinions shows how essential it is for the affiant of the warrant to be able to explain the various technical nuances of the affidavit he or she signed. The opinions make it clear that the defense attorneys in these cases retained technology experts to hyper-analyze every detail of the peer-to-peer process and the investigators were called upon to justify many technological issues. Unprepared investigators and prosecutors can easily create bad case law in this area. Because of the technical nature of the issues presented, I chose to insert direct passages from the opinions where relevant.

Cases:

United States v. Duggar, 2021 WL 4853518 (W.D.Ark., 2021)

Failure to mention Torrential Downpour was used in BitTorrent download did not require a Franks hearing. The probable cause section approved by the court follows:

In May 2019, a HSI Internet Crimes Against Children (ICAC) Task Force affiliate was conducting an online investigation on the BitTorrent Peer-to-Peer (P2P) file sharing network for offenders sharing child pornography. During the course of the investigation, a connection was

> *made between the HSI ICAC Task Force affiliate's investigative computer and a computer/device running BitTorrent software from an IP Address of 167.224.196.113. In May 2019, two separate downloaded files were successfully obtained from IP Address 167.224.196.113. One of the downloaded files was a ".zip" folder containing approximately sixty-five (65) images and the other downloaded file was a single video. The HSI ICAC Task Force affiliate then viewed portions of the downloaded files which were determined to be consistent with child pornography. The device at IP Address 167.224.196.113 was the only IP Address which shared the contents for the files downloaded, and as such, the files were downloaded directly from this IP Address. The HSI Task Force affiliate then determined the IP Address was geo-located to Northwest Arkansas, at which time the lead information and downloads were forwarded to the HSI Special Agent in Charge Office in Fayetteville, Arkansas for further investigation.*
>
> *The above description provides probable cause to believe a crime was committed. The fact that the Task Force affiliate utilized Torrential Downpour to make a connection "between [her] investigative computer and a computer/device running BitTorrent software from an IP Address [assigned to Mr. Duggar]," id., was not necessary to include in the affidavit. Accordingly, the omission of this fact was not material to the probable cause analysis and does not justify a Franks hearing.*

United States v. Boozer, 2021 WL 78865 (D.Or., 2021)

> Minor inconsistencies in affidavit for search warrant did not rise to deliberate falsehoods or reckless disregard for truth and thus defendant was not entitled to *Franks* hearing; agent's statement in affidavit that computer at defendant's IP address was offering to share files of known child pornography, rather than files of investigative interest, was not made deliberately or recklessly, and files did contain child pornography.

United States v. Schwier, 3:17-CR-00095-SLG, 2020 WL 1258027, at *4 (D. Alaska Mar. 16, 2020)

> *For similar reasons, the Court finds that the Franks exception does not apply in this case. Like the affiants in Chiaradio and Maurek, Agent Allison provided a detailed affidavit that disclosed the use of an investigative software program to download a file containing*

> *child pornography from the defendant's computer. He was not required to disclose any as yet unsuccessful challenges to the reliability of Torrential Downpour,[42] nor does the Court find that this omission constituted reckless disregard for the truth.[43] In short, the defense has not made the requisite substantial preliminary showing that Agent Allison's affidavit recklessly omitted key information that, if provided, would have prevented the magistrate judge from finding probable cause.*
>
> *The defense argues that "[b]ecause the affidavit contained absolutely no information establishing the reliability of Torrential Downpour, no officer could have had an objectively reasonable belief that the warrant was based on probable cause."46 The defense relies on United States v. Luong, where the Ninth Circuit held that a sparse affidavit that "relie[d] on an unverified tip" had "no appreciable indicia of probable cause."47 The defense compares Torrential Downpour to an anonymous tip or a dog sniff and contends that "no officer could have an objectively reasonable belief that an affidavit lacking any ... showing [of reliability and/or veracity] establishes probable cause."* The court rejected this argument.

United States v. Arumugam, 2020 WL 1154651, at *4 (W.D. Wash. Mar. 10, 2020)

> In rejecting defendant's request for a Franks hearing, the court noted, "*The Court agrees with the reasoning of these analogous cases, and concludes that any omissions in the affidavit regarding technical details of RoundUp and its automated operations were not material to the probable cause inquiry. Further, the Court concludes that any alleged concerns as to RoundUp's reliability are speculative."*

United States v. Hoeffener, No. 19-1192, 2020 WL 873369 (8th Cir. Feb. 24, 2020)

> District court did not abuse its discretion in denying defendant's request for *Franks* hearing in child pornography prosecution, despite defendant's contentions that police detective exaggerated his descriptions of images obtained from defendant's computer, incorrectly labeled them child pornography when they were actually child erotica, and failed to inform issuing judge that referenced images were not files that law enforcement officers had previously "flagged" as constituting child pornography, where

affiant had personally reviewed images, images were reviewed independently by two officers and both concluded they constituted child pornography, and court found that affiant's descriptions of images were consistent with downloaded files.

United States v. Noden, 2017 WL 1406377 (D.Neb., 2017)

Using Grid Cop software, investigator applied for search warrant of defendant's home. Investigator compared hash values of files advertised by suspect to a CP library of known child pornography. His affidavit, however, falsely stated that he did a browse and direct download from the suspect. The appellate court ruled that it was not a Franks violation because the affidavit supported probable cause after redacting the false information.

State v. Hofman, 2017 WL 977008, at *1 (Ariz.App. Div. 2, 2017)

Detective stated in search warrant affidavit that she downloaded 5 files from suspect's computer. At trial, she said she did not download them, but identified them from comparing hash values. Court ruled in State's favor on *Franks* issue.

Com. v. Hay, 2016 WL 7438672, at *2 (Mass.App.Ct.,2016)

First, the mere possibility that someone else in the neighborhood had used the (unsecured) *WiFi connection emanating from the defendant's residence did not negate the probable cause finding. The residence associated with the IP address was a likely place to find evidence of illegal activity using that IP address.*[3]

Second, the defendant was not entitled to a Franks *hearing, both because (1) the unsecured nature of the WiFi connection was immaterial to the probable cause analysis, and (2) he made no showing, let alone the requisite "substantial preliminary showing," that the affiant had recklessly disregarded the truth in omitting that information.*

United States v. Maurek, No. CR-15-129-D, 2015 WL 5472504, (W.D. Okla. Sept. 16, 2015)

"The Court likewise overrules Defendant's contentions. The material fact law enforcement was obligated to disclose was its use of investigative technology to track, identify, and download the files

> from Defendant's computer. This fact was fully disclosed. More exacting details and disclosures simply were not required to establish probable cause."
>
> Defendant confuses the test for determining the admissibility of evidence from an expert witness at trial under Fed.R.Evid. 702 with the more flexible and less demanding standard for evidence necessary to establish probable cause.

U.S. v. Palmer, Slip Copy, 2015 WL 4139069 M.D.Fla.,2015.

> Agent stated in affidavit that law enforcement "downloaded several torrent files with contained numerous child pornography images and videos." Defendant objected based upon the fact that a torrent files only contains instructions and does not contain actually images. Court said it was not a big deal and denied motion.

U.S. v. Pirosco, 787 F.3d 358 (6th Cir. 2015)

> Defendant failed to make a substantial preliminary showing that an affiant for a search warrant knowingly and intentionally, or with reckless disregard for the truth, included a false statement or material omission in the affidavit, as required to warrant an evidentiary hearing under *Franks* in defendant's prosecution for knowingly receiving and distributing child pornography; defendant's claim that if he had been given a copy of a proprietary program that law enforcement used to download files from defendant's computer that he might have been able to make the preliminary showing was speculative, and the defendant did not dispute that he was a guest at each of the hotels where he used the local wireless network to access child pornography. U.S.C.A. Const.Amend. 4.

People v. Bernal, Not Reported in Cal.Rptr.3d, 2014 WL 4470888 (Cal.App. 6 Dist.):

> The trial court ruled that possibility of someone using suspect's unsecured wireless router did not defeat probable cause for search warrant. This is not a Franks case, but deals with an issue frequently addressed in Franks cases. The case is unpublished and not to be cited, but it contains a review of other cases that came to the same conclusion.

U.S. v. Case, Slip Copy, 2014 WL 1052946 (E.D.Wis.)

Defendant requested a Franks hearing based upon several perceived misrepresentations in a Roundup/Ares search warrant application. The court rejected all of the defendant's arguments.

The three main arguments were:

1. Affiant mislead court by not mentioning use of Roundup and implying data was from a covert person.
2. Agent unlawfully entered defendant's computer.
3. Reliability of program was not established.

State v. Schuller, 287 Neb. 500, --- N.W.2d ----, 2014 WL 684602 Neb., 2014

Detective's failure to explain in search warrant affidavit that the IP address was dynamic and subject to change was not material because the affidavit explained how the same GUID was used during the entire time.

> *And because Schuller repeatedly searched for, downloaded, viewed, and deleted child pornography, we conclude that the evidence was sufficient to support a finding that he knowingly possessed it.*

U.S. v. Thomas, 2013 WL 6000484 (D.Vt.)

The court rejected defendant's multiple claims in motion for Franks hearing, including allegations that detective did not disclose enough info about CPS software and data. The defense also attacked the lack of reliability testing of software, the use of hash values and the use of CP libraries instead of doing direct downloads.

This opinion provides a detailed description of how CPS works and the court destroys the credibility of defense expert Tammy Loehrs.

U.S. v. Thomas, 2012 WL 4892850 (D.Vt.)

During P2P investigation, agent noted that there were several unsecured wireless routers in the apartment complex. The agent failed to include that fact in his search warrant application. The appellate court denied the motion to suppress, stating that there would have been probable cause even if the judge had known about

the unsecured routers. The opinion notes that an unsecured router makes it possible that someone outside the residence was sharing child pornography, but it is still likely that the offender is within the home.

Lefferdink v. State, 250 P.3d 173 (Wyo.2011)

Deputy's misstatement in affidavit as to the date and time he viewed the sharing of pornographic material through defendant's computer internet protocol (IP) address was at most as a result of negligence or a simple mistake, and thus, constituted insufficient grounds to set aside deputy's affidavit in support of search warrant.

Deputy's affidavit in support of request for a search warrant was sufficient to cause a reasonably cautious person to believe the crime of sexual exploitation of children had been or was being committed by the user of the internet protocol (IP) address listed in affidavit, even without the inclusion of a date and time in the affidavit, where the affidavit sufficiently indicated the IP user's identifying information was available, and that evidence of a crime could be found on computers located in that user's residence.

U.S. v. Flyer, 633 F.3d 911 (9th Cir. 2015)

Evidence of corruption of data on defendant's laptop computer, and affiant's statements concerning her inability to download files thought to contain child pornography from defendant's computer due to traffic on defendant's laptop were insufficient to make a substantial preliminary showing that affiant lied when she claimed to have downloaded two images of child pornography from defendant's computer, as required to justify a *Franks* hearing.

Discussion: The investigator was only able to do download one image from the defendant's computer. She stated in her affidavit that she could not download more because of the volume of traffic on the defendant's computer. They later determined forensically that the defendant had configured his software to only allow one download. The court was not overly concerned with this nuance.

U.S. v. Budziak, Slip Copy, 2011 WL 175505 (N.D.Cal.)

Court properly denied defendant's request for a Franks Hearing. Defendant cited a computer article alleging that Limewire created a backdoor in its program that allowed it to remotely manipulate the

software. Defendant alleged that since he disabled file sharing on his Limewire program, the FBI software must have had access to the backdoor. He also argued that since the forensic examiner did not find many of the files allegedly seen by the agent, the agent must have made a misrepresentation.

The court ruled that even if this stuff was true, it would not have defeated probable cause.

U.S. v. Nelson, 2010 WL 2746400 (D.S.D.)

Defendant, who was charged with possession of child pornography, met his preliminary burden of showing that a false statement was recklessly included in the warrant affidavit, which led to a search of defendant's home and car. Therefore, defendant was entitled to a *Franks* hearing. An agent stated in the warrant affidavit that he had received information stating an IP address was subscribed by defendant on the dates and times the agent had inquired about. However, the agent had merely concluded that the defendant was the subscriber based on the information he had received, which never explicitly stated that defendant was the subscriber. Further, there was a one-to-two week discrepancy between the date indicated on the subpoena for the information and the dates on the information the agent had received.

U.S. v. Collins, 753 F.Supp. 2d 804 (S.D.Iowa 2009)):

Law enforcement officers in applying for search warrant for defendant's house did not recklessly or intentionally omit information regarding reliability of software used to locate defendant's IP address as one making child sexual abuse files available for download on peer-to-peer networks, and therefore, defendant was not entitled to a *Franks* evidentiary hearing regarding warrant's probable cause following his indictment on four charges, including distribution of visual depictions of minors engaging in sexually explicit conduct; officers verified information obtained through the software by establishing a direct connection with defendant's computer, gaining a list of available files on defendant's computer, comparing the unique identification file values to values of known visual depictions of minors engaging in sexual conduct, using the IP address to locate defendant's physical residence, completing a records search to identify defendant, and conducting surveillance at defendant's residence.

Search warrants are issued based on the totality of the circumstances indicating that it is fairly probable, not certain, that the contraband will be found at the place to be searched.

Additionally, even if the omitted information had been included in the warrant affidavit, probable cause for the search warrant would still exist.

Discussion: The defense called a computer forensics expert to testify that there is such a thing as a malicious ultrapeer that provides false information. He argued that this should have been explained to the judge in the affidavit. The court noted that the general reliability of Peer Spectre is well established in law enforcement.

U.S. v. Schimley, 2009 WL 5171826 (N.D.Ohio):

Failure to list SHA1 values in search warrant affidavit does not require a Franks hearing.

Failure to mention that a modified version of Phex was used in the investigation does not require a Franks hearing.

U.S. v. Craighead, 539 F.3d 1073 (9th Cir. 2008):

In ruling that the defense was not entitled to a Franks hearing based upon knowingly or recklessly containing false information in the affidavit, the court addressed the following issues:

"Craighead first points to SA Andrews' statement in paragraph 32 of the affidavit that "[t]wo files from IP address 68.0.185.11 were downloaded by your affiant." He contends that this statement impermissibly suggests that the files were downloaded from his computer, when they were never located on his computer. Craighead's claim lacks merit because the statement does not suggest that the files were downloaded from his computer. The statement communicates only that SA Andrews downloaded two files that were listed as available for download from IP address 68.0.185.111. SA Andrews does not aver that the files were found on Craighead's computer."

"Craighead next argues that SA Andrews impermissibly omitted any statements from her affidavit relating to IP spoofing, internet hijacking, and internet theory. His theory, apparently, is that had SA Andrews included this information, the magistrate judge would have understood the possibility that, despite the IP address connection,

the files may not have originated on Craighead's computer. It is true that “deliberate or reckless omissions of facts that tend to mislead” can be grounds for a Franks hearing. United States v. Stanert, 762 F.2d 775, 781 (9th Cir.1985). However, the omission rule does not require an affiant to provide general information about every possible theory, no matter how unlikely, that would controvert the affiant's good-faith belief that probable cause existed for the search. SA Andrews did not commit a misleading omission by failing to omit from her affidavit general knowledge about computer hacking that might support how, hypothetically, Craighead may not have downloaded to his own computer the files that SA Andrews downloaded from Craighead's IP address.”

“Craighead points to SA Andrews' statements about what files were available to download via LimeWire and which files were actually downloaded. In paragraph 32 of the warrant affidavit, SA Andrews stated that she ran a search and “viewed the results of the search and observed multiple files available to be viewed and downloaded by others at IP address 68.0.185.111” and that she downloaded two of these files. In paragraph 33, SA Andrews stated that “[n]umerous other files were also available for downloading from IP address 68.0.185.111” and then listed seven of those filenames as a “sampling.” Craighead argues that SA Andrews impermissibly failed to state that the filenames shown in paragraph 33 were merely text in a search results window and that it was not possible to know whether these files actually existed unless SA Andrews had successfully downloaded them. This argument lacks merit. SA Andrews' statements in these two paragraphs communicate only that her search indicated that numerous files were available for download from the listed IP address. None of SA Andrews' statements in paragraphs 32 and 33 amount to an averment, express or implied, that she knew that all of the files whose names appeared in the search results window actually existed on Craighead's computer. On the contrary, in paragraph 34, SA Andrews expressly stated that she attempted to download one of the files listed in paragraph 33 but was unable to do so because the server was *1082 overloaded. Nowhere did she indicate that she had attempted to download or otherwise verify the location of the other files whose names she listed in paragraph 33.”

U.S. v. Klynsma, Slip Copy, 2009 WL 3147790 (D.S.D.)

Detective’s failure to state in peer-to-peer affidavit that the suspect had a wireless network that could be accessed by others justified a *Franks* hearing.

Since no evidence was presented that detective was aware of the existence of the wireless network, his failure to include the fact did not defeat probable cause.

Discussion: The court ruled that the government did not willfully or recklessly leave out the fact that the defendant used a wireless connection, but left the door open that the issue may be problematic if the defense can establish that making such a determination should have been done.

U.S. v. Flyer, 2007 WL 2051373 (D.Ariz.))

Search warrant affidavit indicated agent downloaded 2 files from defendant's computer. Those files were not found on the computer during forensic exam. Defense expert noted that numerous access dates had been changed after the computer was seized, compromising the integrity of the evidence. Defense requested a Franks hearing, arguing that the two files were never on the computer, but were later placed there by the government. The court rejected this argument and denied Franks hearing.

Defense also argued that agent lied in affidavit by stating the "Need More Sources" message that appeared when she was attempting a download meant that too many people were trying to download files from the defendant. Defense expert testified that it could be the result of many other issues. The court ruled that it was irrelevant to probable cause whether it was truthful or not.

U.S. v. Latham, 2007 WL 4563459 (D.Nev.)

In arguing for a Franks hearing, Defendant argued, that the alleged omissions in the peer-to-peer search warrant affidavit were intentional or reckless because (1) the Cox internet computer connection to which Larry Latham was the subscriber could have been located at premises other than the address shown on the Cox Communication billing records; (2) computer users outside Mr. Latham's residence could have connected to the internet under IP address 68.224.236.152 by accessing the wireless router and modem in Latham's residence; or (3) that it was possible for other computer users, using different IP addresses, to "spoof" or fake the IP address assigned to Larry Latham and make it appear that their internet connections were through the IP address assigned to him.

The court ruled that the affidavit would have supported probable cause even if the three contested facts had been included.

U.S. v. Warren, 2008 WL 3010156 (E.D.Mo.):

> Court properly denied defendant's motion for a Franks hearing. This case involves numerous allegations by the defendant that the Detective included misleading information in the search warrant application. The court covers the affidavit with great detail and analyzes each point separately. The majority of the issues raised concern the fact that the affidavit indicated the defendant was contributing to the distribution of child pornography and that he downloaded at least part of the file from the defendant's computer. At the suppression hearing, the detective testified that he could not be sure that the defendant actually contributed to the multiple source download. The court did not see this as a problem in that the defendant was advertising that he had the file. This language should support historical affidavits in that the court does not appear to think it is necessary to actually download the file.
>
> A person making such use of the video file can reasonably be considered to be a "collector."
>
> "It was the computer's offering to share the video file with child pornography which informed paragraph 6's statement that the subject computer was "contributing to the distribution of child pornography." The subject computer in effect told interested parties on the Internet that it had available for downloading the video file with the SHA1 value of H4V ... UTI. By responding affirmatively to the request for a file with that SHA1 value, the subject computer was in effect stating that it had the entirety of the file, as the search warrant affidavit explained expressly in paragraphs 5, 9, and 14. This was sufficient information to persuade a reasonable person that child pornographic images would be found on the subject computer."

U.S. v. Wiser-Amos, 2008 WL 3494042 (W.D.Ky.)

> Using Bearshare, German authorities did a search for a babyshivid video. The Bearshare program provided a list of IP addresses that contained the file. The German authorities referred the case to ICE and a search warrant affidavit was done in the U.S. The affidavit led the reviewing court to believe that the officer actually downloaded the file, but it was subsequently learned that the officer was unable to do a download.
>
> "While the affidavit does not actually contain false statements or information, the affidavit does omit the information that the

Computer Crime Unit was unable to download the video file in question from the IP address in question on July 13, 2005. This information should have been disclosed to the Magistrate. After a review of the deposition and letter of Officer Klamann, the Court concludes that such omission was in "reckless disregard for the truth." As a result, the Court finds that Defendant has satisfied the first prong of *Franks."*

Even though there was no actual download, there was still a fair probability that evidence of a crime would be located at the premises to be searched. Motion denied.

U.S. v. Hibble, 2006 WL 2620349 (D.Ariz.))

Court denied defendant's motion for a Franks hearing.

Defendant attacked the search warrant based upon the following alleged misrepresentations:

Files Downloaded

Defendant argued that agent could not have downloaded the 2 files she claimed because they were not subsequently found on computer.

Files Available for Downloading

The affidavit was misleading "in that the titles were simply "names" and may have been otherwise empty, deleted, corrupted, or incomplete files unless actually opened, viewed, and downloaded. Moreover, because these files were not found on Defendant's hard drive by Defendant's expert witness they were listed by SA Andrews to 'inflate the issue of probable cause.'"

Attempted Downloading, Parallel Query and Download

Defendant argued that agent's statement in affidavit that she could not download certain files from the defendant's computer because "too many people were requesting" it was misleading because the LimeWire FAQs indicates several other reasons that could account for this. Furthermore, the agent should not have downloaded same file using a parallel query.

In response to these points, the court stated,

> *Defendant argues that there are a myriad of explanations that could account for the images of child pornography in his computer, related devices and media: hacking, "spoofing", tampering, theft, destruction, or viral infections by others. Defendant argues that SA Andrews could have had an internet "chat" to identify the suspect. The Defendant argues that SA Andrews could have investigated further to discover that his neighbor was accessing his open wireless router, although he offers no identifying information as to who this neighbor might be or how he would know that his neighbor had done this. All these issues are more suitably addressed at trial by way of his defense. An affidavit may support probable cause even when the Government fails to obtain potentially dispositive information.*

In reference to the parallel query issue, the court stated, "The circumstances that led to SA Andrews performing a parallel query and download of File 3 is not unlike one obtaining information that Person A has the current month's issue of *Field and Stream* in his home, going to a magazine shop and purchasing that same issue and later finding the same issue in Person A's home."

Reasonable Expectation of Privacy in Shared Folders

Several opinions have addressed this issue and they overwhelmingly favor the government. The investigator should address the defendant's knowledge of the nature of the shared folder in his statement and should have the forensic examiner determine whether the software was configured to share files. It is also helpful to document the installation process of the software used. These same steps will assist in prosecuting the defendant for distribution.

Cases

Youngman v. State, 2022 WL 2374439 (Fla.App. 2 Dist., 2022)

> *In light of the foregoing, the trial court properly concluded that Mr. Youngman lacked a reasonable expectation of privacy in the publicly available electronic files, and the corresponding hash values, shared over BitTorrent. The evidence from the suppression hearing demonstrated that PCSO's CPS software only searched for information that Mr. Youngman's computer made publicly available over the network.*

United States v. Pobre, 2022 WL 1136891, at *7 (D.Md., 2022) **Freenet**

> *In sum, Pobre has not convinced this Court that his Freenet activities are protected by the Fourth Amendment. The LEN captures only that information which Pobre has willingly disclosed to third parties in opennet mode. Nor is there anything particularly sophisticated about law enforcement's software—it simply permits the law enforcement node access to information otherwise available to others in the Freenet space. In that regard, Freenet Roundup bears little resemblance to the enhanced surveillance methods which, by virtue of the technological advantages bestowed on law enforcement, constitute an invasion of a person's reasonable expectation of privacy. Thus, the information obtained from the LEN in this case is not subject to Fourth Amendment protections.*

The case is a good source for how Freenet works and how Roundup's software monitors it.

The case also discuss why Carpenter does not apply to this situation.

United States v. Shipton, 5 F.4th 933 (C.A.8 (Minn.), 2021)

To demonstrate that a police officer, in downloading part of a computer file from a peer-to-peer file-sharing network, had thereby conducted a warrantless Fourth Amendment "search" of communication that was later determined to contain child pornography and to originate from an internet protocol (IP) address associated with defendant, defendant had to show both that he had actual, subjective expectation of privacy in the communication and that his expectation of privacy was one which society was prepared to recognize as reasonable, something which he could not do as to file placed in peer-to-peer file-sharing network.

Defendant has no objectively reasonable expectation of privacy, of kind protected by the Fourth Amendment, in files that he shares over a peer-to-peer network, including those shared anonymously with law enforcement officers

United States v. Arumugam, 2020 WL 1154651, at *4 (W.D. Wash. Mar. 10, 2020)

RoundUp, software with certain technological modifications to a public, open-source P2P network sharing client, is designed to access public files that individuals affirmatively place into the public sphere. Defendant had no reasonable expectation of privacy in the files he chose to upload to his eMule "shared" folder for public download. Accordingly, the government's use of RoundUp to access his public files did not constitute a Fourth Amendment "search."

Defendant has not established any purported "digital trespass" in the government's use of RoundUp, and has not shown that any Fourth Amendment search occurred.

In rejecting defendant's request for a Franks hearing, the court noted, "*The Court agrees with the reasoning of these analogous cases, and concludes that any omissions in the affidavit regarding technical details of RoundUp and its automated operations were not material to the probable cause inquiry. Further, the Court concludes that any alleged concerns as to RoundUp's reliability are speculative."*

United States v. Hoeffener, 2020 WL 873369 (8th Cir. Feb. 24, 2020)

Government's warrantless use of software program (Torrential Dounpour) to identify individuals offering to share or possess files known to law enforcement to contain images or videos of child pornography did not violate defendant's Fourth Amendment rights, despite defendant's contention that his enhanced efforts to protect privacy of his internet communications created reasonable expectation of privacy that might not have existed with other file sharing programs, where government only searched for information that user had already made public through peer-to-peer file-sharing networks.

United States v. Sigouin, 2019 WL 7373045, at *7 (S.D. Fla. Dec. 19, 2019), report and recommendation adopted, No. 9:19-CR-80136, 2019 WL 7372958 (S.D. Fla. Dec. 31, 2019)

Considering all of these factors, Mr. Sigouin has not proven by a preponderance of the evidence that he held an objectively reasonable expectation of privacy in the information that his computer was transmitting and/or making freely available to his neighbors on the Network. See United States v. Ramos, 12 F.3d

1019, 1023 (11th Cir. 1994) (movant bears burden of proving legitimate expectation of privacy in areas searched). The government's warrantless monitoring of that information through the FBI node, even if it involved a physical intrusion into Mr. Sigouin's computer, did not violate the fourth amendment. Suppression is not warranted on this basis.

Mr. Sigouin argues that the Affidavit did not adequately consider or exclude the possibility that persons located outside the physical residence, or who did not reside there, could have accessed the Network through the target IP address. While those scenarios are certainly possible, it was not necessary for the Affidavit to conclusively exclude them.

United States v. Shipton, 2019 WL 5330928 (Minn. 2019) *slip copy*

P2P user had no reasonable expectation of privacy in shared folder.

CPS is a government agent for 4th Amendment analyses.

This very thorough case discusses the Roundup and CPS systems in great detail. The court specifically rejected defense expert Loehr's testimony that the programs search outside the shared folders. The court also found her testimony lacked credibility. The court rejected defense arguments that Carpenter and Jones have created an expectation of privacy when the government uses technology to amass great amount of surveillance.

People v Worrell, No. 1486/12, 2013-06446, 96 N.Y.S.3d 269, 2019 N.Y. Slip Op. 02127, 2019 WL 1272269 (N.Y.A.D. 2 Dept., Mar. 20, 2019)

Defendant had no expectation of privacy in downloaded files depicting child pornography and, thus, search warrant was not required for searching and downloading the files from defendant's computer; files were accessible to anyone who had downloaded peer-to-peer software for free off of the internet.

People v. Martin, 2018 WL 4658755, (Cal.App. 3 Dist., 2018) *unpublished*

No reasonable expectation of privacy in files downloaded with Roundup BitTorrent program.

California ECPA was not violated.

State v. Baric, 2018 WL 4489656, at *4 (Wis.App., 2018)

> *After considering the factors applicable to this case, we agree with the State that Baric did not have an objectively reasonable expectation of privacy in files he publicly shared on a P2P file sharing network. Baric had no property interest in the eDonkey file sharing network, and once he made the files publicly available for download, he did not have any dominion or control over the files. He could not prevent anyone, including law enforcement, from accessing the P2P network and viewing the files that he offered to share.*
>
> *Kyllo does not control our conclusion here because Baric has not shown by a preponderance of the evidence that he had a reasonable expectation of privacy in files he publicly shared for download on a P2P file sharing network.*

Phipps v. Raemisch, 2018 WL 4352007, at *10 (D.Colo., 2018)

> *Consistent with these cases, we hold that Phipps did not have a reasonable expectation of privacy in the files that he made available for public viewing through LimeWire. Because Phipps did not have a reasonable expectation of privacy in those files, his counsel's failure to challenge the search on Fourth Amendment grounds, even if deficient, could not have constituted Strickland prejudice.*

United States v. Landry, 2018 WL 3239284, at *1 (C.A.5 (La.), 2018)

> *There is no reasonable expectation of privacy with respect to IP addresses, or images and information made publicly available in a shared folder on a peer-to-peer network.* United States v. Weast, *811 F.3d 743, 747–48 (5th Cir. 2016). Although Landry alleged that investigators accessed private files that were not in his shared folder, he did not offer any evidence to support that claim. Moreover, the Government's expert witness testified that the software used by investigators in accessing the images was incapable of accessing files not made available for sharing. Accordingly, the district court did not err in concluding that Landry failed to establish a Fourth Amendment violation.*

People v. Worrell, 59 Misc.3d 594 (N.Y.Sup., 2018)

Defendant, in seeking to suppress physical evidence seized after law enforcement officers accessed the content of his home computers, failed to establish that he had a reasonable expectation of privacy in the area "searched," namely, a "shared" folder on his computer which was linked to a peer-to-peer file-sharing program; nature of shared folder was to advertise and distribute the files and their contents to third parties, thereby destroying any expectation of privacy.

Detective's use of Child Protection System (CPS), a software tool which locates Internet Protocol (IP) addresses in a law enforcement officer's jurisdiction which might have child exploitation files, to download images from defendant's computer was not a "search" within the meaning of the Fourth Amendment, and so there was no search of defendant's computer prior to detective's search warrant application; every connection to and interaction with defendant's computer by detective could have been done by a civilian using file-sharing software, CPS merely automated this aggregation of public information as part of the investigative process, and though defendant used a firewall, this did not create expectation of privacy, as he opened door in firewall through use of file-sharing software so as to allow third parties to access contents of his files.

As to the use of CPS in particular, every Fourth Amendment challenge to its use has failed in federal courts, which have repeatedly found CPS to be both a reliable investigative tool and that it does not perform a search of suspects' computers.

Gray v. United States, 2017 WL 6558494 (N.D.Ohio, 2017)

Petitioner had no expectation of privacy in the child pornography that he made publicly available in the shared folder of the peer-to-peer program. Law enforcement officers did not violate the Fourth Amendment by downloading what Petitioner made publicly available.

Shumate v. State, 2017 WL 1149163 (Mo.App. W.D., 2017)

Defendant did not have a legitimate expectation of privacy in computer files shared on a peer-to-peer network, and thus law enforcement's use of Department of Justice website, which was designed to assist law enforcement investigations of child exploitation, during its investigation to determine defendant's internet protocol (IP) address, without a search warrant, did not

violate defendant's Fourth Amendment rights; detective explained at length how defendant's IP address was obtained from the Department of Justice website, and the website searched publicly available information

Rideout v. Clarke, 2017 WL 811492, at *4 (E.D.Va., 2017)

Applying the logic in Borowy to this case, therefore, even assuming without deciding that appellant had the subjective intention to prevent others from accessing his files, appellant still did not have an objectively reasonable expectation of privacy in those files, given his decision to install the Shareaza file-sharing program on his computer. Indeed, appellant installed software on his computer that is specifically designed to share files from one's own computer with other users of that software. By installing the Shareaza peer-to-peer file sharing software on his computer, appellant assumed the risk that other users of Shareaza—including the police—could readily access those incriminating files that could be shared through Shareaza.

People v. Phipps, 2016 WL 7473811, at *4 (Colo.App., 2016)

Indeed, we have found no reported case that has held that a computer owner has a reasonable expectation of privacy in files that he or she makes available through software such as LimeWire.

Court rejected defendant's assertion that he maintained a reasonable expectation of privacy because he was not aware that his files were being shared.

People v. Evensen, 208 Cal. Rptr. 3d 784 (Ct. App. 2016), review filed (Dec. 7, 2016)

Under Fourth Amendment, computer users generally have an objectively reasonable expectation of privacy in the contents of their personal computers, but there are exceptions to this general rule, and one of them is that computer users have no reasonable expectation of privacy in the contents of a file that has been downloaded to a publicly accessible folder through file-sharing software.

Police officers did not violate defendant's Fourth Amendment reasonable expectation of privacy in the files on defendant's computer, in using a computer program that constantly searched peer-to-peer networks for users who were making files known to be child pornography available for download, even if defendant tried to prevent others from accessing files on his computer by changing the settings on the program he used for downloading, since the

officers' program would not have even detected defendant's files if they had never been publicly accessible.

Police officers' information that defendant made child pornography files accessible on a peer-to-peer download network was not too stale to support a search warrant's execution, where defendant had been last seen on the peer-to-peer network four months prior to issuance of the warrant.

United States v. Giboney, No. 4:15CR97JAR (SPM), 2016 WL 873325, (E.D. Mo. Feb. 18, 2016), report and recommendation adopted, No. 4:15CR00097 JAR, 2016 WL 866964 (E.D. Mo. Mar. 7, 2016)

Defendant had no reasonable expectation of privacy in files shared via GigaTribe file sharing account.

U.S. v. Weast, 2016 WL 321329 (C.A.5 (Tex.),2016)

Defendant who used computer to share and download child pornography did not have reasonable expectation of privacy in his internet protocol address or a file shared through a peer-to-peer network, and thus law enforcement's warrantless use of peer-to-peer software to identify defendant's internet protocol address and to download possible child pornography from the file shared by defendant did not violate his Fourth Amendment right to be free from unreasonable search and seizure; defendant voluntarily disseminated his address in the normal course of internet use and made child pornography files publicly available. U.S.C.A Const.Amend. 4

Frazier v. State, 2015 WL 7302669 (Fla. Dist. Ct. App. Nov. 20, 2015)

In ruling that use of CPS software to detect child pornography on peer-to-peer networks did not violate the Fourth Amendment, the court noted,

> *Appellant knew or should have known that sharing files over the Gnutella network would "allow the public at large to access files in his shared folder unless he took steps to avoid it." Borowy, 595 F.3d at 1048. Accordingly, Appellant did not have a reasonable expectation of privacy in the files he shared over the Gnutella network. Because Appellant did not have a reasonable expectation of privacy in*

> *those files, the information gleaned from the CPS software did not constitute an illegal search, and, therefore, formed a valid basis for probable cause to issue a search warrant. For these reasons, the trial court correctly denied Appellant's motion to suppress.*

United States v. Dunning, 2015 WL 5999818 (E.D. Ky. Oct. 15, 2015)

> Defendant did not have reasonable expectation of privacy when he shared files on P2P network.

United States v. Hall, 2015 WL 5897519 (M.D. Fla. Oct. 7, 2015)

> The Magistrate Judge found that Officer Zachary Ewert's warrantless May 9, 2014 search and downloading of images from defendant's computer using Roundup BitTorrent software was not a trespass in violation of the Fourth Amendment. The Magistrate found that, while law enforcement officers used search devices not in general public use, these search devices did not allow law enforcement greater access than the general public to files defendant had made publicly available for sharing. (Doc. # 57, pp 11–16.) Additionally, the Magistrate Judge found defendant did not have an expectation of privacy in computer files which he had made available to others, and any subjective expectation of privacy was not reasonable. (*Id.* at 16.)
>
> Court refused to accepts magistrates findings concerning whether Roundup database was populated with Fourth Amendment violations. Nobody at hearing knew enough about how it worked, so the court said defendant could explore the issue through discovery and readdress it later.

United States v. Maurek, No. CR-15-129-D, 2015 WL 5472504, at *4 (W.D. Okla. Sept. 16, 2015)

> Defendant had not reasonable expectation of privacy when he installed bit torrent program on his computer.
>
> "Where there is no reasonable expectation of privacy over the shared files, the technical aspects of the law enforcement software are not at issue."

Connor v. State, 2015 WL 4450118 (S.D.Ohio, 2015)

Defendant did not have a reasonable likelihood of privacy in shared Limewire files.

"*Conner responds that he did not know the files he downloaded from LimeWire would be publicly accessible. To prove this point, he emphasizes efforts he made to keep these files private by moving them to compact disks and reinstalling his operating system on the computer to "wipe[ ] the hard drive clean." But these efforts only prove that he was ineffective at keeping the files he downloaded from LimeWire from being detected. They do not establish that he was unaware of a risk of being discovered."*

State v. Holland, 272 Or. App. 211 (2015)

Use of Peer Spectre and Shareaza LE did not constitute a search.

State v. Peppin, 186 Wash. App. 901, 347 P.3d 906 (2015)

Detective's use of enhanced peer to peer file sharing software to remotely access the shared files on defendant's computer was not a violation of search and seizure provision of State Constitution; detective's access of defendant's computer through peer to peer software and download of shared files was not a disturbance of defendant's private affairs, defendant voluntarily offered public access to computer files obtained by detective, defendant used peer to peer software to make these shared files available without restriction, anyone wanting to view or download the files could do so, detective's use of specially designed software to search the peer to peer network did not transform his actions into an unlawful search, peer to peer software was not an enhancement device that allowed law enforcement to view what was hidden to the public, and detective did not gain more information than was available to the public.

What is voluntarily exposed to the general public and observable without the use of enhancement devices from an unprotected area is not considered part of a person's private affairs for purposes of Washington Constitution's search and seizure provision.

United States v. Pirosko, 787 F.3d 358 (6th Cir. 2015)

Even assuming that defendant did not waive his right to appeal the trial court's denial of a motion to suppress the result of a search of defendant's shared folder in a file-sharing program in defendant's plea agreement, defendant did not have a reasonable expectation of privacy in data in a shared folder, as files in a shared folder cannot,

by definition, be considered files that an individual expects to be kept private.

State v. Combest, 271 Or. App. 38, 350 P.3d 222 (2015)

Police officers' use of computer software to seek out and download files from defendant on a peer-to-peer network, and to obtain the IP address, GUID, and hash value associated with those files, was not sufficiently intrusive to be classified as a "search," within meaning of state constitutional provision protecting right against unreasonable search or seizure, in prosecution for encouraging child sexual abuse; information that the police had obtained was the same information that was available to any other user of the network, and the police had obtained the information by zeroing in on shared files that contained child pornography, not by engaging in all-encompassing surveillance of defendant's online activity.

Defendant did not retain a privacy interest in information that he provided to network users when he made child pornography files available for download, even if he had expected that no other user would take notice of that information or find it particularly useful, and therefore police officers' access of that information did not violate defendant's state constitutional rights in prosecution for encouraging child sexual abuse.

The fact that technology has created efficiencies or conveniences in police practice does not mean that police conduct a "search" when they use it, within meaning of state constitutional provision protecting right against unreasonable search or seizure.

State v. Roberts, 2015 UT 24, 345 P.3d 1226:

Defendant did not have reasonable expectation of privacy in files shared openly over peer-to-peer network and, thus, law enforcement's use of computer database of digital file values corresponding to files containing child pornography and software that searched files on peer-to-peer file sharing network for identified values was not "search" subject to Fourth Amendment protections; defendant made no effort to limit access to his files on network, and law enforcement database merely enabled officers to recognize files with particular values without allowing access to private information on defendant's computer.

U.S. v. Martinez, 588 F. App'x 741 (9th Cir. 2014)

> *The point of "shared" file is that they can be viewed and obtained by others, meaning that Martinez could not reasonably have expected them to remain private. The use by law enforcement of proprietary forensic software packages that revealed information, such as hash values and IP addresses, did not make the search unlawful, as there was no reasonable expectation of privacy in this information, either. It was available to others, even though they may not have known how to view it.*

State v. Welch, State v. Welch, 236 Ariz. 308, 340 P.3d 387, 389 (Ct. App. 2014), review denied (June 11, 2015)

> *We therefore conclude that Welch, by knowingly using a file sharing network, maintained no reasonable expectation of privacy in the files accessible on that network.*

U.S. v. Westley, Slip Copy, 2014 WL 3545071 (S.D. Ga. July 14, 2014)

> *Westley had files containing child pornography images on the peer-to-peer network eDonkey, and his computer "answered" queries for these images based on keyword searches law enforcement personnel initiated (or which a private citizen could search). As such, Westley had no objective expectation of privacy in those images, and law enforcement personnel were permitted to access these files. Norman, 448 F. App'x at 897 ("even if Norman held a subjectively reasonable expectation of privacy in the shared files on his computer, this expectation was not objectively reasonable. As the record shows, Norman's computer contained a peer-to-peer file-sharing program—which Norman himself used—that allowed other public users of such software to access the shared files on his computer.").*

U.S. v. Dennis, Slip Copy, 2014 WL 1908734 (N.D. Ga. May 12, 2014)

> It does not matter whether shared files are partial downloads or complete downloads, the relevant issue is "whether Dennis had a peer-to-peer file-sharing program that 'allowed other public users of such software to access the shared files on his computer.'"
>
> "ShreazaLE is a law enforcement enhanced program which has no greater access to other users' shared files than any other Gnutella client. ShreazaLE does, however, organize data and download files in a manner that screens for child pornography and creates an evidentiary record."
>
> "So, even if CPS does collect information, it collects publicly available information, which does not run afoul of the Fourth Amendment."

United States v. Hill, 750 F.3d 982 (8th Cir. 2014)

The defendant had no reasonable expectation of privacy in publicly shared files in a peer-to-peer file-sharing program folder on his computer, and thus, police officer did not violate defendant's Fourth Amendment right to be free from unreasonable searches and seizures by accessing defendant's computer using peer-to-peer software and downloading files from defendant's shared folder.

State v. Aguilar, Slip Copy, 2013 WL 6672946 (Tenn.Crim.App.)

Defendant did not have a reasonable expectation of privacy in shared folder.

Standard P2P affidavit and warrant established probable cause to search defendant's home.

Rideout v. Com., 62 Va. App. 779, 753 S.E.2d 595 (2014)

Detective downloaded child pornography from suspect's computer using ShareazaLE. Suspect claimed he tried to disable file sharing and thus had a reasonable expectation of privacy. The court rejected defendant's argument.

Assuming that defendant had subjective intention to prevent others from accessing files on his personal computer by engaging feature of file-sharing software intended to prevent such access, such subjective intention did not create objectively reasonable expectation of privacy sufficient to invoke Fourth Amendment protections with respect to contents of files in his computer, in light of widespread public access granted by file-sharing software; by installing peer-to-peer file sharing software on his computer, defendant assumed risk that other users of such software, including police, could readily access incriminating files that could be shared through such software.

Police did not act in improper manner in obtaining files containing child pornography from defendant's personal computer, such as would warrant application of exclusionary rule as deterrent; parties stipulated that police did not hack into defendant's computer or use any other nefarious means to obtain access, but rather obtained access through modified version of software defendant had downloaded onto his own computer and was using, and officer's affidavit established that he had used only such means as were available to members of the public to access and screen files at issue.

U.S. v. Thomas, 2013 WL 6000484 (D.Vt.)

There is no reasonable expectation of privacy in shared folders.

This opinion provides a detailed description of how CPS works and the court destroys the credibility of defense expert Tammy Loehrs.

State v. Aston, 2013 WL 4746760, La.App. 5 Cir.,2013.

Defendant does not have Fourth Amendment privacy rights in computer files that he or she has shared on file-sharing networks.

Defendant charged with possession of pornography involving juveniles did not have Fourth Amendment right to privacy in contents of his computer, after making such contents available to the world by way of peer-to-peer file-sharing network.

US. v. Franklin**,** 2013 WL 4442030 (W.D.Ark.)

First, the Court finds that use of the Round Up program was not an unconstitutional invasion of privacy.

Second, the Court finds that Eversole's affidavit provided sufficient probable cause for issuance of the March 16, 2012 search warrant.

U.S. v. Dodson, 2013 WL 4400449 (W.D.Tex.) (CPS eDonkey Case)

Government's use of specialized software that identified files on peer-to-peer networks that contained child pornography and located users of those files, to identify defendant as someone who had downloaded and/or distributed potential child pornography, did not constitute an illegal warrantless search within meaning of the Fourth Amendment; Government's software did not actually search the contents of defendant's computer, but only obtained publicly shared information and files.

Defendant had no reasonable expectation of privacy in contents of files he made available for public download from his computer, and thus Government's use of specialized software that identified files on public networks that contained child pornography and located users of those files, to identify defendant as someone who had downloaded and/or distributed potential child pornography, did not

constitute an illegal warrantless search within meaning of the Fourth Amendment.

A user of file-sharing software has no reasonable expectation of privacy, within meaning of the Fourth Amendment, in his publicly shared files because it is not an expectation of privacy that society is willing to recognize.

U.S. v. Hoffman, 2013 WL 3974480 (D.Minn.)

"The knowing use of a file-sharing program defeats any claim of a reasonable expectation of privacy in the files shared on that network."

U.S. v. Brooks, Slip Copy, 2012 WL 6562947, E.D.N.Y.,2012

Officer did not violate defendant's 4th Amendment Rights when he deceived the defendant into inviting him into his Gigatribe account.

"Brooks' attempt to rely on the Supreme Court's recent decision in *United States v. Jones*, —— U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) is misplaced…. In contrast to *Jones*, there is no evidence here that the undercover agent made any physical intrusion on a constitutionally protected area. The agent did not install any device or software on Brooks' computer to enable monitoring or tracking, did not physically enter Brooks' home, and did not physically access his computer."

State v. Dunham, 111 So.3d 1095, La.App. 1 Cir.,2012

Police officer's use of peer-to-peer file sharing technology, which was unavailable to the public, to search defendant's computer did not constitute an illegal, warrantless search; a defendant had no privacy rights in computer files they have on a file sharing network.

Ables v. U.S., 2012 WL 5378815 (S.D.Ohio)

Petitioner had no reasonable expectation of privacy in the peer-to-peer software used by him to access the internet to order to obtain and share child pornography.

U.S. v. Hill, 2012 WL 2735329 (W.D.Mo.):

> The court rejected defendant's contention that E-Phex program constituted illegal hacking. The court ruled that the defendant had no reasonable expectation of privacy in information he voluntarily shared with the network.

Daigle v. State, 2012 WL 1522208 (La.App. 3 Cir.), 2011-1209 (La.App. 3 Cir. 5/2/12)

> In applying for a search warrant for a defendant's home computer, a state police detective did not violate any reasonable expectation of privacy by using software available only to law enforcement to identify a defendant's internet protocol (IP) address as having secure hash algorithm (SHA) values that could be associated with child pornography; defendant had previously elected, when entering a contract with the provider of a file-sharing application, to freely share files having those SHA values with the provider's other clients.

U.S. v. Nolan, 2012 WL 1192757 (E.D.Mo.)

> *The undisputed evidence, however, is that the information was obtained from a "shared" folder that was accessible through a peer-to-peer file sharing program. By participating in peer-to-peer file sharing and placing his files in the shared folder, defendant made the contents of the files available to the police and to anyone else who wished to access them. There is no evidence that the police installed any device or software on the defendant's computer that enabled them to monitor or track his usage.*

U.S. v. Soderholm, Slip Copy, 2011 WL 5444053 (D.Neb.)

> "After careful consideration, I agree with the government that the defendant did not have an objectively reasonable expectation of privacy in the files stored on his computer once he designated those files for sharing with the "friends" on his private network. The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The fact that the defendant's files were restricted to designated "friends" does not alter the fact that the files were no longer kept private, and the defendant bore the risk that the contraband material that he shared with his "friends" would find its way into the possession of law enforcement officers. See Sawyer, 786 F.Supp.2d 1355–56; Ladeau, 2010 WL 1427523, at *5. Because the defendant had no legitimate expectation of privacy in the files that he released to his "friends," the actions of SA Couch—who was a designated "friend"—did not implicate the Fourth Amendment."

U.S. v. Norman, 2011 WL 4551570 (C.A.11 (Ala.))

> Even if defendant convicted of knowingly possessing child pornography held a subjectively reasonable expectation of privacy in shared files on his computer, this expectation was not objectively reasonable where his computer contained a peer-to-peer file-sharing program that allowed other public users of such software to access the shared files on his computer, and thus police officers' warrantless access and search of the shared files did not violate Fourth Amendment.

U.S. v. Stallans, 2011 WL 3206076 (E.D.Tenn.)

> Defendant did not have expectation of privacy in folder he chose to share with others.

U.S. v. Conner**,** 2011 WL 3359570 (S.D.Ohio)

> "Each court that has considered this issue has held that an individual does not have a reasonable expectation of privacy in data files that are shared with the public through peer-to-peer software."
>
> "Assuming that Defendant had a subjective expectation in privacy in the information, that subjective expectation is one that society and the law is not prepared to recognize. A person has no legitimate expectation in privacy in information he voluntarily turns over to third parties."

U.S. v. Sawyer, 2011 WL 2036444 (N.D.Ohio) **Gigatribe Case**

> The defendant did not have an objectively reasonable expectation of privacy in the files that he shared over the Internet using a "closed" peer-to-peer file sharing program, with which other users that the defendant had accepted as "friends" could browse, search, and download files stored in the defendant's shared folders, and thus, the defendant did not have a Fourth Amendment privacy interest in the materials stored on his computer that were shared using the file sharing program.
>
> The defendant's consent to a government agent's search of files that the defendant shared over the Internet using a "closed" peer-to-peer file sharing program, with which other users that the defendant had accepted as "friends" could browse, search, and download files stored in the defendant's shared folders, was not rendered

involuntary, for Fourth Amendment purposes, by the government's use of a ruse, in which the agent used the account of a person the defendant had designated as a "friend," to obtain access to the materials stored on his computer that were shared using the file sharing program.

Even if defendant had a Fourth Amendment privacy interest in the materials stored on his computer that were shared using a "closed" peer-to-peer file sharing program, with which other users of the program that the defendant had accepted as "friends" could browse, search, and download files stored in the defendant's shared folders, another user of the file sharing program who had been designated as a "friend" by defendant gave effective third-party consent to a government search of defendant's shared files by giving a government agent consent to use his program account for purposes relating to an official investigation.

U.S. v. Gabel, 2010 WL 3927697 (S.D.Fla.,2010)

The Undersigned agrees with every other federal court to have addressed this issue, and finds that users of peer-to-peer networks do not enjoy a reasonable, objective expectation of privacy in the files they share. The Undersigned also agrees with the Ninth Circuit's view in Borowy that law enforcement's use of a computer program which allows them to confirm whether the files contain child pornography has no bearing on whether defendants possess a legitimate expectation of privacy in those pornographic files. Any of the hundreds of thousands (or millions) of users on the Gnutella network could have searched for Gabel's shared files and downloaded those files exclusively from Gabel. That is exactly what law enforcement did here.

The enhanced programs merely permitted law enforcement to more easily organize and classify information that was otherwise available to the public, which aided them in obtaining evidence to support a search warrant. Gabel had no reasonable expectation of privacy in his files. He was, essentially, sharing them with the entire world. Anyone with internet access could have easily downloaded Gnutella client software, logged onto the network and downloaded Gabel's files. The fact that law enforcement did so with a device that enabled them to screen for child pornography and collect data for evidentiary purposes does not alter the privacy analysis or in any way shroud Gabel with the Fourth Amendment's protection. It simply means that the police were doing their job. The tool used by law

> *enforcement here is no different, from a constitutional perspective, than the myriad special means-street cameras, radar and canines-that police legally use every day without prior judicial approval to efficiently gather evidence by accessing public information. These police tools do not generate Fourth Amendment concerns because they do not access anything which the public cannot access. Thus, law enforcement's use of an enhanced computer program is the digital equivalent of a pole camera, which is legal and which does not require a warrant or court order.*

United States v. Norman, 2010 WL 3825601 (M.D.Ala.):

> Defendant did not have a reasonable expectation of privacy in his Limewire shared folder.

U.S. v. Stults, 575 F.3d 834 (8th Cir. 2009)

> Defendant lacked a reasonable expectation of privacy in files on his personal computer which were accessible to others for file sharing based on his installation and use of peer-to-peer file sharing software, and thus federal agent's use of file-sharing program to access child pornography files on defendant's computer did not violate defendant's Fourth Amendment rights; even if defendant did not know that others would be able to access files stored on his own computer, defendant knew he had file-sharing software on his computer.
>
> "The information contained in the affidavit shows that, through the P2P file-sharing program, Agent Cecchini was able to access and download files directly from Stults's computer that contained child pornography images. As a result, a fair probability existed that contraband would be found at Stults's residence in his personal computer."
>
> Quote: *One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking.*

U.S. v. Ganoe, 538 F.3d 1117 (9th Cir. 2008):

> The defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, and thus, agent's use of file-sharing software program to access child pornography files on the computer did not violate defendant's Fourth Amendment rights;

> defendant had installed and used file-sharing software, thereby opening his computer to anyone else with the same freely available program, and defendant had been explicitly warned before completing the installation that the folder into which files were downloaded would be shared with other users in the peer-to-peer network.
>
> "The crux of Ganoe's argument is that he simply did not know that others would be able to access files stored on his own computer. But he knew he had file-sharing software on his computer; indeed, he admitted that he used it-he says to get music. Moreover, he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network. Ganoe thus opened up his download folder to the world, including Agent Rochford. To argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes."

U.S. v. Brese, 2008 WL 1376269 (W.D.Okla.)):

> The Court finds that, notwithstanding any subjective expectation that Defendant may have had in the privacy of his computer, it was not reasonable for him to expect privacy in files that were accessible to anyone else with LimeWire (or compatible) software and an internet connection. This is not unlike the personal computer that the defendant in United States v. Barrows, 481 F.3d 1246 (10th Cir.2007), networked to a workplace computer for the purpose of sharing files. The court of appeals stated that, even though the defendant invited no one else to use his computer and may have expected its contents to remain private, "his failure to take affirmative measures to limit other employees' access makes that expectation unreasonable."

U.S. v. Borowy, 2010 WL 537501 (9th Cir. 2010):

> Defendant did not have objectively reasonable expectation of privacy in files on his computer that were publicly accessible due to his having installed publicly available peer-to-peer file-sharing computer program, even though he had attempted to engage feature of program software that allowed user to prevent others from downloading or viewing names of files on his computer, and thus, FBI agent did not violate Fourth Amendment by logging onto program and using keyword search to locate the files; defendant knew he had installed file-sharing program that would allow public

to access files in his shared folder unless he took steps to avoid it, and despite his efforts, his files were still entirely exposed to public view, and anyone with access to file-sharing program could download and view them.

Even if FBI agent's action of downloading and examining files that he found on defendant's computer using a publicly available peer-to-peer file-sharing computer program that defendant had installed on his computer constituted a seizure of those files, the agent had probable cause for that seizure; file names for at least five of the files were explicitly suggestive of child pornography, and list of these file names was obtained by logging on to the file-sharing program and searching for term known to be associated with child pornography, and agent used software program that verified hash marks of files and displayed red flag next to known images of child pornography, and two of defendant's files were red-flagged as known child pornography.

U.S. v. Meysenburg, WL 1090664 (D.Neb.)

The defendant did not have standing to challenge the warrantless search of the shared files where the defendant did not have a reasonable expectation of privacy in them. A police officer searched shared files from a file sharing program on the internet. He located child pornography and was able trace the files back to the defendant.

State v. Thornton, 2009 WL 3090409 (Ohio App. 10 Dist.)

Appellant knowingly exposed to the public the files found on Perry's computer and the IP address associated with that computer through the use of the Limewire program on the computer. Therefore, he had no reasonable expectation of privacy in that evidence.

U.S. v. Ladeau, 2010 WL 1427523 (D.Mass.) **Gigabribe**

Defendant does not have a reasonable expectation of privacy in the folders he chooses to share in Gigatribe, even if he limits access to certain people.

Does File Sharing Constitute Distribution?

Most of the opinions indicate that a defendant can be charged with distribution of child pornography by placing it in a shared folder on a peer-to-peer client. The prosecution should be prepared to prove that the defendant knew others could take files from his computer and some courts require at least a partial download from the defendant. Documenting the installation process of the software and doing

screen captures of the software interface with the various options chosen will assist in proving the defendant knew he was distributing files.

Cases

United States v. Clark, 2022 WL 203026, (C.A.6 (Ky.), 2022)

> Knowing-distribution element of defendant's child pornography conviction was satisfied through circumstantial evidence that defendant knowingly distributed illegal images and videos when he placed them in accessible public folder on peer-to-peer network; fact-finder reasonably could have inferred that defendant knew that placing child pornography in his shared folder meant that it could be accessed and downloaded by others, including law enforcement, user could have turned off program's default sharing function and defendant did not take any such steps, and defendant set up two evidence destruction programs on his computer to run at computer's start.

United States v. Pratt, 2021 WL 5918003, at *2 (C.A.9 (Ariz.), 2021)

> *The government presented enough evidence at trial and sentencing for the district court to conclude that Pratt knew of the uTorrent program's peer-to-peer file-sharing capabilities. Even though Pratt initially claimed ignorance about the ability of other users to access his downloaded files, he admitted to being knowledgeable about computers generally and to using a software program called Tor to access the "dark" web, as well as websites like Pirate Bay, a file-sharing search engine. These admissions, together with other circumstantial evidence in the record, were enough to support the district court's finding that Pratt knew of uTorrent's file-sharing capabilities. Indeed, evidence of a defendant's "technical knowledge and familiarity" with a file-sharing program can be enough to establish that the defendant "knowingly" distributed child pornography.*

United States v. Owens, 18 F.4th 928 (C.A.7 (Wis.), 2021)

> It is criminal "distribution" of child pornography to knowingly make a file containing child pornography available for others to access and download via a peer-to-peer file-sharing network.

Jeror v. State, 2021 WL 631623, (Fla.App. 2 Dist., 2021)

> *We agree that the State presented sufficient evidence through the detective's testimony that would allow the jury to find beyond a reasonable doubt that Jeror reasonably should have known that the child pornography files would be accessible to and transmitted to others through his use of the wTorrent program and the peer-to-peer network. The trial court did not err in denying Jeror's motion for judgment of acquittal, and we affirm Jeror's judgment and sentence.*

The detective downloaded child pornography from the defendant's computer using BitTorrent. A subsequent search of the defendant's computer did not discover any illicit images, but there were numerous programs that showed he had advanced computer skills. He had wiping software, VPN software and software designed to access the dark web. The court's ruling was primarily based on the language in the transmitting child pornography statute that says, "knew or reasonably should have known that he or she was transmitting child pornography."

Schoen v. State, 2023 WL 3964011 (Tex.App.-Dallas, 2023)

Unsophisticated P2P user who routinely moved files out of his shared folder was not guilty of possession with the intent to promote.

United States v. Ruiz-Castelo, 2020 WL 6482170, at *1 (C.A.9 (Ariz.), 2020)

Defendant argued the government failed to present evidence that he viewed the CP video in the 45 minutes between his successful P2P download and the completion of the agent's download from defendant's computer. The court rejected this argument by stating,

> *But the government was required to prove Ruiz-Castelo's knowledge that the video contained sexually explicit conduct with a minor, not that Ruiz-Castelo necessarily viewed the video before he distributed it.* United States v. X-Citement Video, Inc., 513 U.S. 64, 78, 115 S.Ct. 464, 130 L.Ed.2d 372 (1994). *The government provided sufficient evidence to the jury for it to conclude beyond a reasonable doubt that Ruiz-Castelo knowingly distributed child pornography. The government provided ample evidence that (1) child pornography files are often named*

> *so that users know they contain child pornography, (2) "lola" is one of the names commonly used to signal a file contains child pornography, and (3) Ruiz-Castelo was a frequent user of child pornography. Combined with the evidence that Ruiz-Castelo was well-acquainted with how the file-sharing network BitTorrent works and frequently used it to download child pornography, the jury had more than sufficient evidence to convict him of knowing distribution of child pornography.* United States v. Budziak, 697 F.3d 1105, 1109–10 (9th Cir. 2012).

United States v. Clarke, 979 F.3d 82 (C.A.2 (N.Y.), 2020)

> Defendant's knowing participation in peer-to-peer file-sharing network to receive child pornography images, which implicitly invited other network participants to download files from defendant's computer, constituted "knowing" transportation of child pornography, as element of defendant's conviction for transportation of child pornography; while defendant asserted that it was government agents downloading images from his computer that caused transportation of such images without defendant's explicit awareness, transportation of child pornography from defendant's computer to others was an almost inevitable consequence of his participation in file-sharing network.

United States v. Massillon, 2020 WL 5778387, at *4 (A.F.Ct.Crim.App., 2020)

> *The Government introduced evidence that the very nature of BitTorrent, which Appellant evidently sought out and installed, was to share downloaded files across the network. Furthermore, Appellant almost certainly used the BitTorrent user interface repeatedly, and that interface would have informed Appellant that his files were being uploaded. In addition, as described above, in order to install the BitTorrent program, Appellant would have seen a screen that informed him he was installing a "peer-to-peer file distribution application"—even if he did not then scroll down to read the "Automatic Upload" section explicitly informing him he was enabling others to upload the files he downloaded. Thus, the military judge was presented with substantial circumstantial evidence that Appellant knew he was sharing child pornography through the BitTorrent network.*

United States v. Flores-Rivas, 2020 WL 3525534 (N.M.Ct.Crim.App., 2020)

Military judge did not abuse his discretion in finding that there was an adequate factual basis for accused's guilty plea to specification of knowingly distributing child pornography and in accepting the plea; accused stipulated to his installation, on his personal laptop where child pornography was stored, of peer-to-peer file-sharing software that enabled other users of the software to download pornography from his laptop, just as he had downloaded such pornography from other computers with same software, that he was aware of what software did, and that he realized that others were downloading child pornography from his laptop, though he was unaware of the exact time and place of such downloads.

Mason v. State, 2020 WL 975362 (Tex. App. Feb. 28, 2020)

Defendant properly convicted of possession with the intent to promote child pornography when he had the images in his shared folder.

United States v. Cullen, 2019 WL 6211211, at *3 (C.A.11 (Fla.), 2019)

Generally, courts should be cautious in their approach to distribution charges brought in the peer-to-peer software context. Peer-to-peer software runs on the sharing of downloaded files. If users do not proactively disable all sharing upon installing the software, their files will be shared indefinitely without their awareness and even when they have stepped away from their computer. The software also intentionally makes it difficult for the average user to manage which of their files are being shared at any given moment, often obscuring instructions for disabling sharing, as is the case with Shareaza. Given the nature of this software, courts should focus with particular care on whether distribution on peer-to-peer software was done knowingly.

United States v. Waguespack, 2019 WL 3820068 (C.A.5 (La.), 2019)

Evidence was sufficient to support conviction for knowingly distributing child pornography; government presented evidence that peer-to-peer file sharing software was installed on computer in defendant's room, defendant was sole user of computer, software

notified users when files were being uploaded or downloaded, software's default settings for shared folder were changed, defendant had advanced technological proficiency, law enforcement agent downloaded child pornography using software from IP address in defendant's home, user on computer previously searched for, viewed, downloaded, and transferred child pornography using software, and computer seized from defendant's room contained over 2800 images of child pornography.

Downloading child pornography from a peer-to-peer computer network and storing it in a shared folder accessible to other users on the network is prohibited under child pornography statute, but the government must prove beyond a reasonable doubt that the defendant engaged in such distribution knowingly.

Evidence was sufficient to support conviction for knowingly possessing child pornography; government presented evidence that there were over 2800 child pornography images on computer seized from defendant's room, person using computer was well-educated in computer usage, defendant was sole user of computer, anti-forensic and encryption software were discovered on computer, child pornography was transferred to law enforcement agent from IP address at defendant's home, and path files with names indicative of child pornography were stored on computer.

State v. Morrill, 2019 WL 3765586, at *7 (N.M.App., 2019) *unpublished*

File sharing is distribution.

State v. Franco, 2019 WL 2559725 (N.M.App., 2019)

There was substantial evidence that defendant intentionally kept files containing child pornography in a shared folder, which were accessible to others, on a peer-to-peer file-sharing network, as required to support his conviction for distribution of child pornography; evidence established that defendant downloaded a peer-to-peer file-sharing network, that defendant was familiar with file-sharing networks generally, that for over five years, defendant used such networks to access child pornography, that defendant used a network that required sharing in order to continue accessing files, and that defendant was sharing his files.

United States v. Neiheisel, 771 Fed.Appx. 935 (C.A.11 (Fla.), 2019)

Sufficient evidence supported finding that defendant knew he was sharing files, or that they were automatically distributed to peer-to-peer network, as required for conviction for distribution of child

pornography; child pornography charged in indictment was shared via peer-to-peer network that was connected to internet protocol (IP) address registered to defendant at address where he resided during charged dates, and although no traces of child pornography were found on defendant's tablet, a communication protocol for peer-to-peer file sharing had been installed on device, and agents testified that defendant had admitted that he had downloaded child pornography, namely, videos charged in indictment, and stored them in shared downloads folder connected to peer-to-peer network.

United States v. Moran, 771 Fed.Appx. 594 (C.A.6 (Ky.), 2019)

Evidence was sufficient to establish that defendant's internet search for child pornography produced a file link to peer-to-peer file sharing program, which defendant activated knowing that he would receive child pornography in his shared download folder, supporting conviction for distribution of child pornography, despite contention that defendant sometimes received content he did not want; evidence included that defendant used file sharing networks, understood that any downloaded files in shared folder could be retrieved by others on network, and knew that child pornography was downloaded to his computer, that defendant admitted to having clicked on child pornography, and file names were consistent with defendant's stipulation that they contained child pornography.

State v. Fodrini, 570 S.W.3d 170 (Mo.App. E.D., 2019)

Sufficient evidence existed that defendant was sophisticated user of peer-to-peer file sharing computer program and was knowledgeable about its file-sharing capabilities, to support finding that defendant knowingly shared child pornography files downloaded from program as required for conviction for promoting child pornography in the second degree, even though program automatically shared downloaded files; program installation process instructed users how to manually change settings to turn off file-sharing feature, defendant admitted installing program and using program for four to five months to search for and download child pornography, and thumb drive seized from defendant's residence revealed 4,200 images and 27 videos of child pornography.

Redkovsky v. State, 240 Md.App. 252 (Md.App., 2019)

Evidence was sufficient for a jury to reasonably find that, based on defendant's understanding of peer-to-peer computer file sharing programs, and his use of a program which made files on his laptop computer available for other users to download, that he knowingly transferred four videos depicting child pornography to a state computer, as required to support his convictions for distribution of child pornography; defendant was a savvy computer user who, as a hobby, repaired broken computers and built a customized desktop computer with multiple hard drives, and defendant admitted downloading and installing the program required for using a peer-to-peer file-sharing network, and indicated that he understood that peer-to-peer file-sharing programs worked by uploading files from one computer and making them available for others to download.

United States v. Romero–Medrano, 2018 WL 3746549 (C.A.5 (Tex.), 2018)

Downloading images and videos containing child pornography from a peer-to-peer computer network and storing them in a shared folder accessible to other users on the network can constitute illegal distribution of child pornography, but to obtain a conviction, the government must prove beyond a reasonable doubt that the defendant engaged in such distribution knowingly.

United States v. Sosa-Pintor, 2018 WL 3409657, at *3 (C.A.5 (Tex.), 2018)

Sosa-Pintor argues that, unlike the defendant in Richardson*, he was not a computer technician. And at trial he argued that he did not know how computers worked and that he was not tech-savvy. Moreover, unlike the defendant in* Roetcisoender*, Sosa-Pintor asserts that he never made any direct admissions that he knew the contents of his ARES shared folder were available to others. He never created any suggestive file names. And the government did not present evidence that Sosa-Pintor had been aware of any warnings presented by the software upon installation.* See United States v. Vazquez*, 623 F. App'x. 716, 717 (5th Cir. 2015).*

Sosa-Pintor's contentions are unavailing. Although he was not a computer technician, sufficient evidence was presented to the jury demonstrating that Sosa-Pintor knew enough about ARES and computers generally to support the verdict that Sosa-Pintor knowingly distributed child pornography through the shared folder. And, contrary to Sosa-Pintor's assertions, he did seem to

acknowledge to the officers during the raid that he understood how the ARES sharing folder worked.

Maddox v. State, 2018 WL 3135227, at *6 (Ga.App., 2018)

Here, Maddox admitted that he downloaded the ARES program onto his computer and that he understood that file sharing was the purpose of that program. He also admitted that he had child pornography stored in his computer's shared folder. Additionally, Maddox could have, but did not, move his downloaded images and videos into a computer folder that was not subject to file sharing. And Cobb County police were able to download images and videos from the child pornography collection in Maddox's shared folder. Under these facts, the evidence supported the factfinder's conclusion that Maddox had distributed child pornography.

United States v. Carroll, 886 F.3d 1347 (C.A.11 (Ga.), 2018)

Evidence was insufficient to prove that the defendant knew he was sharing child pornography files when they were automatically placed in a shared folder on a peer-to-peer network that defendant accessed, as required to support conviction for knowing distribution of visual depictions of minors engaged in sexually explicit conduct; government presented no evidence of defendant's awareness that the downloaded child pornography images were shared with others on the network or that defendant intended or authorized the sharing, as the peer-to-peer program did not prompt the user to choose to share the downloaded files, but did so by default.

Evidence was sufficient to prove that defendant knowingly possessed child pornography found on his computer, as required to support conviction for knowing possession of visual depictions of minors engaged in sexually explicit conduct; government presented evidence that child pornography was regularly downloaded to defendant's computer over an 11-month period, that obtaining the files required predicate manual acts of downloading a peer-to-peer file sharing program, searching for files, and initiating file downloads, that defendant lived alone and had exclusive control over his computer during most of that time period, that his computer was used to download child pornography on the same day it was used to file his tax return, and that defendant was traveling without internet access during a notable gap in the child pornography downloads.

United States v. Ryan, 885 F.3d 449 (C.A.7 (Ind.), 2018)

Defendant who knowingly makes child pornography on his computer available for others to access and download via peer-to-peer sharing has "distributed" child pornography, as that term is used in statute making it unlawful to "knowingly receive[ ] or distribute[ ]" such pornography.

Finding that defendant had knowingly distributed child pornography, in violation of criminal statute, was sufficiently supported by evidence that child pornography on his computer could be downloaded via peer-to-peer sharing, that law enforcement officer had actually downloaded such pornography before warrant was sought for search of defendant's home, and that defendant had sophisticated understanding of computers and software.

People v. Robles-Sierra, 2018 WL 1247579 (Colo.App., 2018)

Prosecution's theory of statutory term "distributes" with reference to defendant's use of peer-to-peer file sharing computer software as element of crime in prosecution for sexual exploitation of a child, arising from defendant's downloading and file sharing of child pornography, was legally sufficient; defendant downloaded hundreds of files of child pornography in a way that made the new file on his computer downloadable by others using the same file sharing software, he had not chosen the option to prevent downloads from automatically being saved in the sharable folder, and other users of such software had downloaded hundreds of defendant's files.

People v. Yedinak, 2018 WL 357279 (N.Y.A.D. 3 Dept., 2018)

Sufficient evidence supported defendant's convictions for promoting a sexual performance by a child, where defendant had knowledge of content and character of images he downloaded to his file sharing program folder, defendant knowingly logged into the file sharing program and used program extensively to download pornography, and defendant knew how program worked generally, and that program was a peer-to-peer file sharing program.

United States v. Stitz, 877 F.3d 533 (C.A.4 (N.C.), 2017)

Defendant's use of peer-to-peer file sharing program constituted "distribution," for purposes of distribution of child pornography; FBI agents downloaded child pornography from defendant's shared

folder, and defendant admitted that he knew his files were being shared.

Kelley v. Clarke, 2017 WL 6210500, (W.D.Va., 2017)

Kelley has repeatedly stated that he never shared child pornography; he only downloaded, viewed, and then deleted the files. However, even though Kelley may have only "passively" allowed other Ares users to download child pornography off of his computer, he used the program, understood the program,[5] and allowed his computer system to facilitate further downloading of child pornography materials by others when he did not deactivate the "sharing" functionality.

United States v. Laurie, 2017 WL 5611300 (D.Minn., 2017)

There is no evidence that Laurie did not know how to use Gigatribe, the peer-to-peer file sharing service that was found on his computer, nor is there evidence that he was not the one who installed Gigatribe. Rather, the evidence at trial supported a reasonable inference that Laurie knew Gigatribe was on his computer, knew how to upload images to Gigatribe, and knew how to share those images with others by providing them with a password. This is more than sufficient to show that Laurie's "use of the peer-to-peer-file-sharing network made the child pornography files in his shared folder available to be searched and downloaded by other [file-sharing] users."

United States v. Furman, 867 F.3d 981 (C.A.8 (Minn.), 2017)

Evidence was sufficient to support defendant's convictions for knowingly distributing child pornography; while defendant stated that he immediately moved or deleted files containing child pornography from his shared folder on file-sharing networks for child pornography, he also indicated that he knew how to access shared folders of other network users and knew how to download other users' files, and he also knew that other users could download files from his shared folders because when he downloaded material, it went into his share file which then shared it back to other users if he did not immediately move or delete it, and police officers were able to download child pornography files from defendant's computer through the file-sharing network.

United States v. Johnson, 694 Fed.Appx. 753, 754–55 (C.A.11 (Fla.), 2017)

> *The district court did not err by determining that Johnson knowingly distributed child pornography when he made files available to other users on a peer-to-peer file-sharing program and a law enforcement officer downloaded the files. See Grzybowicz, 747 F.3d at 1309. Testimony shows that he understood how the file sharing program worked and that by keeping files in his shared folder, without disabling *755 sharing, allowed others to access and download the files. Johnson had in fact disabled sharing on three files. The fact that the agent used a law enforcement version of the file sharing program is of no matter because the Government only needed to prove that Johnson made the files accessible, and, as the district court found, the Government would have been able to download the same images even if it had used the commercial version of the file sharing program. The district court found that it did and Johnson has not undermined the district court's finding. Accordingly, we affirm.*

United States v. Jones, 2017 WL 914253, at *1 (E.D.Mich., 2017)

> Keeping CP images in shared folder of Ares program was sufficient for advertising CP and distribution of CP.

State v. Miller, 2017 WL 1228814, at *5 (N.J.Super.A.D., 2017)

> *The judge found it "inescapable that [ ] defendant would have known ... [t]hat in his files, in his default shared folders, with his having downloaded the peer-to-peer system, that it was available to other people." Accordingly, the State's evidence sufficiently supported the offense charged as defendant acted to "offer" his downloaded child pornographic images and videos by making them available through peer-to-peer file sharing, thereby allowing others on the network to access and copy them.*

Kovach v. Commonwealth, 2016 WL 7094215 (Va. Ct. App. Dec. 6, 2016)

> Similarly, in this case, appellant knowingly downloaded and used the peer-to-peer sharing software on his desktop. Appellant admitted to downloading movies and adult pornography using Shareaza, showing he knew how to use the software. Appellant also admitted that he had accidentally downloaded child pornography in the past. It was reasonable for the factfinder to conclude that appellant should have known that the software had the ability to share files with other users. Appellant's assertion that

> he did not know that the sharing feature was operating is insignificant.

State v. Land, 2016 WL 5404320 (S.C. Ct. App. Sept. 28, 2016)

> Evidence was sufficient to show that defendant knowingly distributed or exchanged pictures or videos of a minor engaged in a sexual act, so as to support conviction for second degree sexual exploitation of minor; in addition to the evidence found on his computer, defendant's own statements established that he solicited the child pornography by using such terms as “pre-teen” and “Lolita” in conjunction with file sharing network to find pornographic images and videos of minors, evidence, including defendant's own admissions, established that defendant knew how file sharing network worked and knew that the child pornography he downloaded would be available for others to download and view, and he admitted to soliciting and downloading multiple pornographic files.

Leita v. State, 2016 WL 6541843 (Tex.App.-Corpus Christi, 2016)

> *Assuming without deciding that evidence of the use of Shareaza and its default protocol alone is not sufficient to establish that Leita knew he was sharing or intended to share or promote child pornography, we conclude that the State presented sufficient circumstantial evidence to establish the challenged knowledge element of this offense. The circumstantial evidence supports the reasonable inference that Leita knowingly shared the significant amount of child pornography he downloaded from Shareaza with others.*

State v. Land, 2016 WL 5404320, (S.C.App., 2016)

> *Land's knowing use of a program with the specific function of downloading and sharing stored files, in conjunction with his acknowledged use of the file-sharing program to download and view the images of child pornography, required that the circuit court deny his motion for a directed verdict.*

Olt v. United States, 2016 WL 3556927 (N.D.Tex., 2016)

Court rejected defendant's assertion that "merely placing a file in a shared computer folder using peer-to-peer software does not meet the legal definition of "transporting or shipping,"

United States v. Johnson, 2016 WL 3221854 (S.D. Fla. June 8, 2016)

This Court has carefully reviewed the above-cited authorities and like the Tenth Circuit concludes that for the purposes of 18 U.S.C.§ 2252(a)(2) an individual has knowingly distributed child pornography if he or she maintains a "shared destination file," has a reasonably sophisticated understanding of peer-to-peer file sharing for the purpose of obtaining child pornography, and law enforcement actually downloads images of child pornography from that file using the peer-to peer-file sharing program.

United States v. Bui, 2016 WL 770191 (11th Cir. Feb. 29, 2016)

Evidence established that defendant acted knowingly in distributing child pornography; defendant's shared folder on GigaTribe peer-to-peer file-sharing network contained over 100,000 child pornography files available for his network "friends" to download, for someone to gain access to defendant's child pornography files he had to have become defendant's "friend" via invitation, an undercover Federal Bureau of Investigation (FBI) employee downloaded 105 child pornography files from defendant through network after being authorized to access defendant's shared folder, and defendant was actively running network's file-sharing program on his computer at time of search warrant.

U.S. v. Vazquez, 2015 WL 8527334 (C.A.5 (Tex.),2015)

Defendant who admitted that others could download files kept in his Ares shared folder could be convicted of distribution of child pornography.

U.S. v. Roetcisoender, 2015 WL 4072103 C.A.5 (Tex.),2015

Evidence was sufficient to support jury finding that defendant knew that child pornography stored in "Incoming" folder of peer-to-peer file-sharing program on his computer was available for sharing with other program users, as required to support conviction for distributing child pornography; defendant generally understood how the program operated, had downloaded and stored over 100,000 images and 2,000 videos depicting child pornography on two

computers and other devices, knew how to move files between the devices, had used internet to access child pornography for over a decade, had used the program for about nine months, and had titled subfolder he created on the program "Young nudists," indicating the contents of the folder and containing terms that those seeking child pornography might use to search for files, yet he gave non-descript titles to other folders on his computer.

U.S. v. Pirosco, 787 F.3d 358 (6th Cir. 2015)

Evidence is sufficient to support a conviction for distribution of child pornography when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it.

U.S. v. Brown, 2015 WL 2215899 (C.A.9 (Nev.))

Evidence that defendant, the proprietor of computer business with substantial technical computer knowledge, had designated non-default folder on his external hard drive to permit peer-to-peer sharing of child pornography on his computer was sufficient to support his conviction of transporting child pornography, such that retrial upon this charge was not barred after his convictions were set aside based on structural error in denial of his right to discharge retained attorney.

United States v. Stephens, 2015 WL 2062220 (A.F.Ct.Crim.App.)

In ruling that sharing files on the eDonkey network as sufficient for distribution, the court observed,

The appellant contends, however, that the evidence does not prove he knowingly distributed child pornography. The appellant argues one matter in particular. According to the record of trial, the eMule peer-to-peer program used by him to collect child pornography had certain security settings. One of those settings was titled "See My Shared Files/Directories" and offered three choices: Everybody, Friends only, and Nobody. At the time the appellant's laptop was seized by the AFOSI, the selected setting was Nobody. This, according to the appellant, demonstrates that, rather than knowingly sharing the child pornography possessed by him with other Internet users, he sought to hide it from others. ***We are not persuaded****.*

Kelley v. Commonwealth, 771 S.E.2d 672 (Va. 2015)

> Evidence was sufficient to support conviction for distribution of child pornography; defendant chose to download file-sharing software onto his laptop computer by which he voluntarily participated in peer-to-peer file-sharing of child pornography, and whether defendant's shared folder containing the child pornography was created as a default option by the software or by defendant himself, the child pornography files were, in fact, downloaded by defendant into his shared folder, and thereby made available to other users of filed-sharing program.

United States v. Stephens, M.J., 2015 WL 2062220 (A.F.Ct.Crim.App.)

> Investigator's downloading of 4 files from defendant's shared folder was sufficient to show distribution. (eDonkey)
>
> *"According to the record of trial, the eMule peer-to-peer program used by him to collect child pornography had certain security settings. One of those settings was titled "See My Shared Files/Directories" and offered three choices: Everybody, Friends only, and Nobody. At the time the appellant's laptop was seized by the AFOSI, the selected setting was Nobody. This, according to the appellant, demonstrates that, rather than knowingly sharing the child pornography possessed by him with other Internet users, he sought to hide it from others. We are not persuaded."*

United States v. Williams, 2014 WL 7476216 (A.F.Ct.Crim.App.)

> In ruling that keeping files in your Ares shared folder was sufficient to support distribution of child pornography, the court stated,
>
> > *In the case before us, the appellant specifically sought out and knowingly possessed files containing child pornography. He then kept these files in a location where the plain language of the program's user agreement indicated others would have access to those files. We see no legal insufficiency where the only evidence of distribution was that a law enforcement agent downloaded the files the appellant made available.*

People v. Gonzalez, 2014 WL 7237517 (Ill.App. 1 Dist.)

> *By downloading the files from the peer-to-peer network and saving them to his hard drive, defendant created digital copies of those*

*files. He then made those copies—which were not previously available on the peer-to-peer network—available for other users to download by saving them in his shared file. According to the State's evidence, defendant admitted knowing that he was making these copies available to other users on the network by saving them in his shared file. Defendant's argument that he did not intend to "make * * * available" those files for download is thus unavailing. 720 ILCS 5/11–20.3(f)(ii) (West 2010). We conclude that, viewing the evidence in the light most favorable to the State, the State proved that defendant possessed child pornography with the intent to disseminate it beyond a reasonable doubt.*

U.S. v. Husmann, 2014 WL 4347186 (C.A.3 (Pa.))

Defendant's action in placing child pornography materials in shared folder available to other users of file sharing network did not constitute "distribution" within meaning of federal statute criminalizing distribution of child pornography, where there was no evidence that anyone accessed, viewed, or downloaded files from his shared folder.

U.S. v. Laub, Not Reported in F.Supp.2d, 2014 WL 1400669 (D.Kan.)

"Defendant argues that his use of Shareaza did not constitute distribution; and, that he did not have the requisite intent of knowingly distributing child pornography files. The Court finds beyond a reasonable doubt that the use of Shareaza constituted distribution and that Defendant used Shareaza with the knowledge and intent to distribute child pornography to other users."

U.S. v. Baker--- F.3d ----, 2014 WL 552753C.A.5 (Tex.),2014.

That defendant allegedly did not know that his use of file-sharing program permitted other users to download child pornography from his computer did not preclude application of sentencing enhancement for distribution of child pornography following his guilty plea to receiving material involving the sexual exploitation of a minor; enhancement applied to any act related to transfer of child pornography, it did not require express mens rea, and defendant's use of program, whether knowingly or not, contributed to proliferation of illicit material, increasing harm to exploited children.

U.S. v. Baldwin, --- F.3d ----, 2014 WL 657949 (C.A.2 (Vt.))

> A District Court's determination that a defendant should have known that his files containing child pornography would be shared by his peer-to-peer (P2P) file-sharing software and that it was almost self-evident that distribution would take place through the P2P software did not constitute a finding that the defendant knowingly distributed child pornography, as required to impose two-level sentence enhancement for distribution of child pornography.

U.S. v. Richardson, 713 F.3d 232 (5th Cir. 2013):

> As an issue of first impression, defendant's actions in storing images and videos containing child pornography in shared folder accessible to other users on peer-to-peer computer network constituted distribution, as required to convict defendant for distribution of child pornography; defendant was a computer technician with computer experience, he affirmatively downloaded peer-to-peer file sharing program and downloaded images and videos from that program's network, he maintained 144 videos in his shared folder, he knew that others could access the materials stored in folder, and police officer actually downloaded one such video.

Biller v. State, 2013 WL 1234222 (Fla.App. 5 Dist.):

> Defendant's conduct of allowing access to computer files of pornographic images of children through a peer-to-peer sharing network did not constitute "transmitting" child pornography, as necessary to support a conviction for transmission of pornography by electronic device; statute setting forth the offense was susceptible of more than one construction, such that, under rule of lenity, statute was to be construed in defendant's favor.

U.S. v. Gorski, 71 M.J. 729, Army Ct.Crim.App.,2012.

> Accused, who placed and maintained electronic files containing child pornography in a shared folder accessible to others via a peer-to-peer file-sharing software program, could not be convicted of "distributing" child pornography under federal statute criminalizing the distribution of child pornography or clauses one or two of Article 134 where there was no evidence that a third party actually downloaded or obtained accused's contraband files.

U.S. v. Cremer, Slip Copy, 2012 WL 6681700, S.D.N.Y.,2012.

> *This conclusion follows from the plain meaning of the term distribution: to give out, dispense, or disperse to others. It is possible to distribute something by making it available to others in*

a manner that invites them to dispense it to themselves. And it is possible to do just that through a peer-to-peer file sharing program. As Judge Gorsuch analogized in Shaffer, a self-service gas station "distributes" gas even if its employees don't hold the pump for customers.

U.S. v. Budziak, 697 F.3d 1105 (9th Cir. 2012)

Evidence supported jury's finding that defendant distributed files containing child pornography by maintaining them in a shared folder accessible to other users of his software, despite his assertion that he disabled the sharing function on the software; he did not present evidence of that assertion to the jury, and the government presented evidence that file-sharing was enabled on defendant's software when they seized his computer, that there were multiple files containing child pornography in his shared folder, and that he initially told law enforcement agents that he had not changed the default settings on the software, and a reasonable jury could have found beyond a reasonable doubt that defendant's technical knowledge and familiarity with the software demonstrated that he knew he was sharing files.

Evidence is sufficient to support a conviction for "distribution" of child pornography when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it.

U.S. v. Caparotta, 2012 WL 3893741 (E.D.N.Y.)

Under plain meaning of "distribute," defendant's placing of child pornography files in shared folder accessible to others via peer-to-peer Internet file-sharing program constituted distribution, for purposes of statute criminalizing distribution of child pornography, even though defendant did not transfer files to a specific person, and FBI agent who accessed defendant's shared folder and discovered child pornography files there had to download files from shared folder before possessing or viewing them, and even though agent could download files without defendant's knowledge or active participation, because by actively placing the files in shared folder, defendant deliberately distributed to all users of peer-to-peer program access to those files and forfeited control over who downloaded them.

People v. Rowe, 2012 WL 2045752 (Colo.App.), 2012 COA 90

> *Reading the plain language of the statute and construing the term "offer" according to its common usage, we hold that a defendant "offers" sexually exploitative material by making it available or accessible to others. In the context of a* ***peer-to-peer*** *file sharing network, a defendant offers sexually exploitative material by knowingly leaving it in the share folder for other users to download. See United States v. Sewell, 513 F.3d 820, 822 (8th Cir.2008) ("In the context of [a* ***peer-to-peer*** *sharing] program, placing a file in a shared folder with descriptive text is clearly an offer to distribute the file."); see also United States v. Lewis, 554 F.3d 208, 211 (1st Cir.2009) ("any file a user downloads through LimeWire is automatically placed in that 'Shared' folder and is therefore offered by that user for further downloads by other users").*

U.S. v. Collins, 642 F.3d 654 (8th Cir. 2011)

> Evidence supported jury finding that defendant had requisite intent to support his conviction for attempted distribution of child pornography, where defendant downloaded and installed file–sharing program onto his two computers, he was knowledgeable about computers, and pictures of child pornography were taken with defendant's cell phone and then stored on one computer and external hard drive.

U.S. v. Ferguson**,** Not Reported in M.J., 2011 WL 1343191 (N.M.Ct.Crim.App.)

> Defendant challenged his plea to attempted distribution of child pornography, stating that he only enabled file sharing to increase his download speed and had no specific intent for others receive any of it. The court ruled that his act of designating the relevant folder as "shared" while knowing others had access to it was enough to support the plea to attempted distribution.

State v. Lyons**,** --- A.3d ----, 2010 WL 4823676 (N.J.Super.A.D.)

> Appellate court ruled that evidence was sufficient to support conviction of distribution of child pornography based upon the fact that defendant had the images in his shared folder. The court rejected defendant's argument that he simply accepted the default settings of the file sharing program, but made no efforts to affirmatively share files.

United States v. Peacock, Slip Copy, 2010 WL 4741133 (C.A.11 (Fla.))

> The district court was entitled to find that Peacock distributed child pornography and that he failed to prove he lacked the intent to distribute that material. The record establishes that Peacock downloaded to his computer images and videos of child pornography that he made fully accessible for other users of LimeWire and some of those materials were transferred on at least one occasion. Peacock argues that he did not "take[ ] any positive step to distribute any images," but Peacock understood that his files would be shared and he restricted access to some of his files, but not those files containing child pornography.

United States v. Frakes, Slip Copy, 2010 WL 4540306 (C.A.10 (Kan.))

> Appellate court ruled that evidence was sufficient sustain a conviction for distribution of child pornography based upon the following:
>
> > *At trial, the government introduced testimony indicating: (1) Frakes stated he knew there was child pornography on his computer; (2) he stated that if there was any child pornography on his computer it was his; (3) he installed Limewire on this computer; (4) he knew the files in his Limewire "shared" folder would be shared with others; (5) his Limewire "shared" folder contained child pornography; and (6) a detective was able to access images of child pornography from Frakes' computer via Limewire.*

U.S. v. Abston, Slip Copy, 2010 WL 4367124 (C.A.10 (Okla.))

> Defendant who had enabled peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to child pornography stored on his computer, had no reasonable expectation of privacy that was violated when federal agent used this peer-to-peer file-sharing program to download images from defendant's computer, and defense attorney did not behave in constitutionally deficient manner in not filing meritless motion to suppress such evidence.

State v. Tremaine, 315 S.W.3d 769 (Mo.App. W.D. 2010)

> Evidence was sufficient to support finding that defendant was aware he was operating his computer in a way that made files containing child pornography available to other users, assuming such

awareness was necessary to sustain a conviction for promoting child pornography in the first degree by offering to disseminate it based on defendant's use of computer file-sharing program; defendant apparently knew the files he possessed would be available for sharing with others, evidence indicated software on defendant's computer was set to allow sharing of files from folder in which child pornography found, evidence indicated that other file-sharing software users had actually accessed files in folder containing child pornography, defendant indicated a working knowledge of the file-sharing software, defendant had made inconsistent statements regarding his level of familiarity with software, and there was no evidence anyone else had unmonitored access to defendant's computer.

U.S. v. Shaffer**,** 472 F.3d 1219 (10th Cir. 2007):

Defendant "distributed" child pornography when he downloaded pornographic images and videos from a peer-to-peer computer network and stored them in a shared folder on his computer accessible by other users of the network; defendant transferred and dispersed the child pornography to others, in that he freely allowed them access to his computerized stash of images and videos and openly invited them to take or download those items, and defendant understood that the purpose of the shared folder was to allow others to access items he stored in it.

Quote: We have little difficulty in concluding that Mr. Shaffer 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 items. 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 or her 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'etre 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.

U.S. v. Dodd**,** 598 F.3d 449 (8th Cir. 2010): *sentencing issue*

> Absent concrete evidence of ignorance, a fact-finder may reasonably infer that a defendant knowingly employed a file sharing program for its intended purpose, namely, to distribute, in determining whether to enhance a defendant's base offense level for offenses involving distribution of child pornography.

U.S. v. Craig**,** 67 M.J. 742 (2009):

> Accused's guilty plea to distribution of child pornography was improvident, where it was supported only by facts that computer images and videos of child pornography were made available for download by others in file-sharing folder on accused's computer, and there was no evidence that anyone actually did so such that the charged distribution resulted in a completed transfer of the contraband.

U.S. v. Sewell, 513 F.3d 820 (8th Cir. 2008)

> Defendant's use of peer-to-peer file-sharing program, called Kazaa, by placing file containing child pornography in shared folder with descriptive text, was "offer" to distribute child pornography, as required for sufficiency of indictment by alleging essential element of offense of knowingly making or causing to be made any notice offering to distribute child pornography, since purpose of Kazaa was to allow users to download each other's files, and purpose of descriptive fields was to alert users to pornographic content of downloadable files.
>
> "In the context of the Kazaa program, placing a file in a shared folder with descriptive text is clearly an offer to distribute the file. To fit this situation within the Tenth Circuit's apt analogy, see Shaffer, 472 F.3d at 1223-24, a Kazaa file's descriptive fields are like a roadside sign to a self-serve gas station at which the owner need not be present to distribute fuel to passing motorists. 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 to them."

U.S. v. Ober, 66 M.J. 393 (2008):

> Evidence that accused used peer-to-peer file sharing network to download child pornography from other participants in file sharing network to his computer, thereby causing an upload on host user's

computer, was legally sufficient to support finding that accused was guilty of transporting child pornography in interstate commerce, considering accused's confession to agents, expert testimony regarding files found on accused's computer, and testimony regarding underlying investigation of accused.

U.S. v. Schade, 318 Fed.Appx. 91, 2009 WL 808308 (C.A.3 (Pa.)

Evidence that undercover police officer downloaded child pornography video through peer-to-peer file-sharing network in part from defendant's computer was sufficient to support conviction for transporting or aiding and abetting the transportation of child pornography, even if there was no way of knowing which portion of the downloaded file was contributed by defendant's computer.

Evidence that defendant was notified while downloading software for peer-to-peer file-sharing network that it would allow others to upload files from his computer, that he changed the default settings for file-sharing, and that he used the software for file-sharing, was sufficient to show that defendant knew child pornography files on his computer could be downloaded by other users, as required for conviction of transporting child pornography.

Interesting quote: *He points out that there is no way of knowing which portion of the downloaded file was contributed by his computer, and thus whether that portion actually depicted a minor engaged in sexual conduct. This argument is unavailing; at the very least Schade is liable as an aider and abettor. His computer contributed some part of a video that showed a minor engaging in sexual activity. It would be eminently reasonable for the jury to have concluded that Schade aided and abetted the transportation of a visual depiction of a minor engaged in sexual activity by making the child pornography file available in the "My Downloads" folder for any part of it to be downloaded, resulting in the utilization of that file by another user of Bearshare seeking to download the complete video.*

U.S. v. Handy, 2009 WL 151103 (M.D.Fla.) :

In ruling that possession child porn images in a shared folder of a peer-to-peer client may constitute distribution, the court compared the shared folder to a self service gas station where the owner advertises his product and lets people take what they want. The court ruled, however, that the government failed to show that the software was actually configured to allow people to share the relevant files.

Quote: *We have little difficulty in concluding that [the defendant] 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 to access to his computerized stash of images and videos and openly invited them to take, or download, those items. 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 all. And neither the owner nor his or her 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 ... 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'etre of owning a gas station is to do just that. So, too, a reasonable jury could conclude that [the defendant] welcomed people to his computer and was quite happy to let them take child pornography from it.*

U.S. v. Abraham, 2006 WL 3052702 (W.D.Pa.):

In ruling that the defendant was properly convicted of distribution of child pornography when an officer downloaded an image from his shared folder, the court stated,

> "The Defendant chose to share the movie image in question with anyone using the Gnutella network via the Bearshare file-sharing program which he installed on his computer. His act of choosing to share the movie image was voluntary on his part. He did not have to share the movie image; the Bearshare program allowed him the option not to share any file he downloaded. Neither the fact that the Defendant did not personally know Trooper Erderly nor the fact that Trooper Erderly had not had any communication with the defendant prior to downloading the child pornography is relevant."

Wenger v. State, 2009 WL 1815781 (Tex.App.-Fort Worth):

Evidence was sufficient to establish that defendant disseminated child pornography so as to support conviction for promotion of child pornography; officers both testified about how their investigations resulted in finding child pornography files stored in subfolders within defendant's "Shared" folder on his computer,

officer explained process of searching for child pornography on peer-to-peer file sharing software and described how he retrieved indicted files from defendant's computer by downloading them to his computer, and other officer confirmed that his forensic investigation revealed that defendant's computer contained same files and user-created subfolders discovered by officer's earlier investigation.

Evidence was sufficient to establish intentional and knowing dissemination so as to support conviction for promotion of child pornography; although defendant claimed that he did not know "how to not share and share and separate those items out," defendant admitted that he knew peer-to-peer file sharing software shared his files, that he assumed users downloaded files from him, and that purpose of software was to allow users to "pull files from members," officer's testimony showed that defendant did at some point before state seized his computer change default software settings so that program did not automatically share defendant's downloaded files, which proved that he did know how to "not share and share" files, and officer stated that software rewarded users for allowing others to download files from his computer, because more files user shared, faster user could download other files.

State v. Tremaine, 315 S.W.3d 769 (Mo.App W.D. 2010)

Evidence was sufficient to support finding that defendant was aware he was operating his computer in a way that made files containing child pornography available to other users, assuming such awareness was necessary to sustain a conviction for promoting child pornography in the first degree by offering to disseminate it based on defendant's use of computer file-sharing program; defendant apparently knew the files he possessed would be available for sharing with others, evidence indicated software on defendant's computer was set to allow sharing of files from folder in which child pornography found, evidence indicated that other file-sharing software users had actually accessed files in folder containing child pornography, defendant indicated a working knowledge of the file-sharing software, defendant had made inconsistent statements regarding his level of familiarity with software, and there was no evidence anyone else had unmonitored access to defendant's computer.

U.S. v. Pires, 2011 WL 1288256 (C.A.1 (Mass.)

Government had no burden to prove that defendant convicted of attempted receipt of child pornography knew that the downloaded file actually contained such images; rather, the government was required to prove that the defendant believed that the received file contained such images.

Evidence was sufficient to support defendant's conviction of attempted receipt of child pornography; jury heard testimony from two FBI agents confirming that, by his own admission, defendant deliberately used terms associated with child pornography when searching on file-sharing program, that defendant admitted that he had an interest in child pornography and had looked at child pornography three or four times a week, downloading five to six images containing child pornography once or twice a week.

General Probable Cause Issues

United States v. Fiore, 2021 WL 165089, at *6 (D.Vt., 2021)

Investigator downloaded single child pornography image from BitTorrent. A search warrant was executed 46 days later. Defense argued the warrant was stale because a single image does not qualify defendant as a collector. It could have been an inadvertent download The court ruled the complex series of steps necessary to get the download were sufficient to show suspect was looking for it and there was no staleness problem.

Jones v. State, 2020 WL 5056118, at *10 (Tex.App.-Dallas, 2020)

An investigator from the Russian Ministry located child pornography being shared from an IP address in the U.S. He forwarded his findings to Interpol, who in turn forwarded it to U.S. officials. Defense argued the ensuing search warrant should be suppressed because the tip from the Russian Ministry was unreliable. In upholding the warrant, the court stated,

> *The failure of the affidavit to identify a specific person from the Russian Ministry or INTERPOL that first viewed the images and the absence of any allegation of prior reliability of either the Russian Ministry, INTERPOL, or a specific person does not render the affidavit defective or insufficient for purposes of establishing probable cause. The United States and Russia are both member countries of INTERPOL that "work together and with the General Secretariat to share data related to police investigations" and are part of a global*

> *network of police along with 192 other member countries. https://www.interpol.int/en/Who-we-are/Member-countries (last visited August 27, 2020). That fact alone provided the magistrate with strong indicia of reliability regarding the information received from the Russian Ministry and INTERPOL.*

Jones v. State, 2020 WL 5056118, at *10 (Tex.App.-Dallas, 2020)

Jones v. Clark County, Kentucky, 959 F.3d 748 (C.A.6 (Ky.), 2020) (*Liability Case)*

> Probable cause existed to make arrest for promoting sexual performance by a minor under Kentucky law, notwithstanding that charges were eventually dismissed, where police tracked source of child pornography video being shared through peer-to-peer file sharing network from device associated with internet protocol address of a wireless router that was in arrestee's apartment, no one else was in the apartment when police arrived, arrestee's router was password protected, and he was the only one with the password.
>
> Note: This is an interesting case discussing federal Civil Rights liability of officers making arrests on P2P case. The police tracked a child pornography video to suspect's residence, executed the warrant and arrested him on the spot. No contraband was found at the scene. A subsequent forensic examination did not reveal any evidence either. After spending a couple of weeks in jail, the charges were dropped. If law enforcement is inclined to make an arrest even though evidence was detected at the scene, they should be familiar with the issues in this case.

United States v. Rees, 957 F.3d 761 (C.A.7 (Ill.), 2020)

> Officer's affidavit provided probable cause to issue search warrants for defendant's apartment, house, and truck for evidence of child pornography; although investigation began with suspicion that suspect device was associated with child pornography or child erotica, which was not contraband, affidavit described how officer connected his computer to the device and compared infohash of files downloaded by the device over peer-to-peer sharing network to infohash of child-pornography files in law enforcement database, tracked geographic location of device's internet protocol (IP) address to defendant's apartment, saw that law-enforcement database indicated same network user had shared child-pornography

at the apartment and defendant's house, and defendant's truck was seen at both residences.

Information in officer's supporting affidavit concerning downloads of child pornography over peer-to-peer sharing network to device associated with defendant's apartment six months prior was not stale and thus could support search warrants for defendant's apartment, house, and truck for evidence of child-pornography; information about downloads was supported by more recent peer-to-peer activity that suggested the same kind of criminal activity had continued, and affidavit confirmed that devices and operating systems involved in peer-to-peer sharing allowed users to retain access to child-pornography files, while also allowing officers to re-cover information about network activity even after a user deleted specific files or had kept a device in storage for months or years.

The court rejected the following arguments by the defense:

> *Specifically, Rees points out that anyone at the apartment complex could have downloaded the October 2017 payload that Officer Lynn's computer reported was located on the suspect device. He adds that Officer Lynn did not actually open the files downloaded in October 2017; the officer instead compared the payload's infohash to that of files in a reference library. Rees also asserts that the affidavit did not clarify that the law-enforcement database includes only information about files that officers have recognized contain child pornography. He reasons that Officer Lynn first described a "peer-to-peer database" and then referred to the "ICAC Cops database" when charting his investigation; the affidavit did not explicitly state that the two terms refer to the same database—the *769 one Officer Lynn described as storing information on the sharing of child pornography. Rees additionally reminds us that child erotica, which may have prompted Officer Lynn's initial inquest into the suspect device's activities, is not contraband. He continues that Officer Lynn did not personally view the files shared in the peer-to-peer activity that officers tied to Rees's apartment and house, specifically. And he lastly urges that the criminal activity Officer Lynn observed in October was stale by the time he applied for the affidavits six months later… These are strong reasons why Officer Lynn had not proven, in the affidavit, that Rees received and possessed child pornography in his apartment, house, and truck. But probable cause is a low bar that can be cleared without a* prima facie *showing of criminal activity.*

State v. McNutt, 303 Or. App. 142 (2020)

Affidavit in support of warrant to search defendant's home computer contained sufficient allegations to support finding of probable cause to believe child pornography would be found on computer; detective with extensive background in investigating child sexual abuse personally viewed 300 files downloaded from defendant's computer using peer-to-peer (P2P) file sharing network and concluded that files showed sexually explicit conduct involving children in violation of encouraging child sexual abuse statutes, file names implied files originating from defendant's computer contained child pornography, including forms of sexual conduct that could be assessed objectively, and defendant's P2P network was frequently used to trade child pornography.

United States v. Rees, 19-2230, 2020 WL 2071942 (7th Cir. Apr. 30, 2020)

Officer's affidavit provided probable cause to issue search warrants for defendant's apartment, house, and truck for evidence of child pornography; although investigation began with suspicion that suspect device was associated with child pornography or child erotica, which was not contraband, affidavit described how officer connected his computer to the device and compared infohash of files downloaded by the device over peer-to-peer sharing network to infohash of child-pornography files in law enforcement database, tracked geographic location of device's internet protocol (IP) address to defendant's apartment, saw that law-enforcement database indicated same network user had shared child-pornography at the apartment and defendant’s house, and defendant's truck was seen at both residences.

Owens v. State, 2019 WL 5996385 (Tex.App.-Texarkana, 2019)

Officer's warrant affidavit provided a substantial basis by which the magistrate could reasonably find there was a fair probability that child pornography would be found at defendant's residence; Internet Protocol (IP) address provided was the one that shared child pornography, Internet Service Provider (ISP) provided information showing that the IP address provided belonged to defendant, defendant was a registered sex offender, and the customer address for the provided IP address matched the appraisal district records showing that defendant owned the home containing the computer with the provided IP address.

United States v. Gonzalez, 2018 WL 6174202, at *4 (S.D.Tex., 2018)

> Possession and distribution of a single video of child pornography may be sufficient to establish probable cause in support of an application for a search warrant.
>
> *Deliberate measures taken by the user to obtain illicit material via the peer-to-peer network and then share it with others indicated intent to obtain and distribute this particular file. Such calculated actions—which go beyond simply accessing illicit material—suggest a tendency to collect child pornography and justify a finding of probable cause.*
>
> *Accordingly, obtaining, possessing, and distributing a single file on two separate occasions is sufficient to establish probable cause.*
>
> *Defendant contends this lacks necessary details regarding (1) how peer-to-peer networks were utilized in this case, (2) how the investigation started, (3) whether the investigative software was automated, and (4) whether the software was successful in prior investigations. (Dkt. No. 22 at 23–24.) Such specificity is not necessary. Requiring this additional information exceeds the threshold to establish a "substantial basis for concluding that a search would uncover evidence of wrongdoing."* Allen, 625 F.3d at 835.

Lewis v. State, 2018 WL 4924936, at *6 (Tex.App.-Corpus Christi, 2018)

> Search warrant affidavit was sufficient to support probable cause under the following circumstances:
>
> > *In his affidavit, Agent Erickson details how he identified a particular IP address sharing known child pornography files. Agent Erickson learned from the internet service provider controlling the IP address that the address was tied to appellant's residence. Agent Erickson viewed video files shared by the IP address and confirmed that they were child pornography. He then visited the residence and discovered that it had a secured wireless network. A vehicle parked at the home was registered to appellant. Agent Erickson also talked to appellant and confirmed that he resided at the home with his wife and daughter.*

Mardosas v. State, 2018 WL 4762753, at *1 (Fla.App. 1 Dist., 2018)

Detective did a Roundup search warrant. He was unable to do a direct download, so he used a description of a video he found in the database. The court ruled that fellow officer rule allowed him to use this description to establish probable cause for the warrant.

People v. Worrell, 59 Misc.3d 594 (N.Y.Sup., 2018)

Ample probable cause supported issuance of search warrant for defendant's home computers; in affidavit in support of search warrant, detective explained his extensive training and experience in investigating internet-based peer-to-peer networks which share child exploitation videos and images, as well as his investigation of defendant, in which he, inter alia, discovered "hash values" on defendant's Internet Protocol (IP) address that matched known child exploitation files and successfully downloaded from defendant's files two images that were determined to be child pornography.

United States v. Morrow, 2018 WL 572506, (W.D.Tex., 2018)

Morrow specifically takes issue with the affidavit's failure to divulge the nature of the computer software used to identify the target IP address. He contends that without disclosing this information to the magistrate judge, there was no way for the probable-cause determination to take into account the reliability or other features of that software.[3] Again, because this omitted investigative detail is not even close to being material or dispositive on the probable-cause determination here, it cannot justify the suppression of evidence.

United States v. Sherlock, 2018 WL 287862 (M.D.La., 2018) *slip opinion*

Court criticizes the bare-bones affidavit submitted, but says there was enough for good faith. It is a bit difficult to interpret the court's opinion, but it appears the detectives listed three names consistent with child pornography and said at least one had a hash value of known child pornography. It appears the detectives neither viewed nor described the actual files.

U.S. v. McKinion, 2017 WL 3137574 (C.D.Cal., 2017)

Court ruled motion to suppress was properly denied based on the following:

> *McKinion argues that the Affidavit failed to establish probable cause because it was based upon an "untenable chain of inferences." Mot. at 9. Specifically, defendant argues that the Affidavit required the magistrate judge to infer or assume that:*
>
> *(1) the law enforcement P2P network/database Rodriguez used (which we now know was CPS) reliably logs the activity of IP addresses in Los Angeles County;*
>
> *(2) that the SHA1 values identified by the CPS database reflected child pornography rather than partial, incomplete, corrupted, or empty files logged by the P2P software;*
>
> *(3) that the NCMEC and LAPD databases reliably maintain accurate information about SHA1 values and associated files; and*
>
> *(4) that there was a fair probability that the sailboat would have evidence of child pornography even though the suspected file-sharing detected by the CPS software had occurred five to eight months earlier.*

The court addressed each of these points and explained how they did not defeat probable cause. The court also denied a request for a *Franks* hearing.

The primary challenge was based on an affidavit from defense expert, Tami Loehrs. She described how SHA1 values located on the computer don't necessarily mean the complete file is present in a viewable state. The court ruled that based on the number of files and the file names, there was probable cause one way or the other.

State v. Arth, 2017 WL 2836073, at *4 (Minn.App., 2017) *unpublished opinion*

Police downloaded a file on P2P network in June 2009 from a specific IP address. They noticed his GUID was continuing to advertise CP from different IP addresses until May of 2010. In denying the motion to suppress, the court stated the following:

> *Although the .212 IP address was last online in June 2009, the computer with GUID DAAF7 continued to access and download child pornography in May 2010. The computer had been placed behind a firewall device and was reporting only its internal IP address to the **peer-to-peer** network. The supporting affidavit for the search warrant stated that child-*

> *pornography collectors "often maintain their collections, in a digital or electronic format, in a safe, secure, and private environment, such as a computer and/or surrounding area;" that "[c]ollectors highly value their collections and often maintain them for several years;" and that "[c]ollectors frequently keep their collection close by, usually at their residence to enable them to easily view the collection."*
>
> *The supporting affidavit showed that (1) the IP address known to officers in March 2009 connected the computer with GUID DAAF7 to Arth as the account holder and to his apartment address, (2) the same computer was still being used to download child pornography in May 2010, and (3) Arth still resided at the same address. Given the nature of the child-pornography crime, this information supports an inference that Arth was continuing to use the computer at his residence to collect child pornography but was attempting to conceal his activity. Considering the totality of the circumstances, the information in the warrant application and supporting affidavit was sufficient to support the district court's probable-cause determination. See State v. Brennan, 674 N.W.2d 200, 206–07 (Minn. App. 2004) (concluding that, due to the expected use and storage of child pornography as described in the warrant application, sufficient nexus existed to support a warrant to search the suspect's home, even though discovery of child pornography had been limited to his work computer).*

United States v. Blouin, 2017 WL 3485736, at *2 (W.D.Wash., 2017)

> *Defendant's contention that law enforcement was required to obtain a search warrant before deploying RoundUp eMule lacks merit, and as a result, his motion to suppress was denied.*
>
> *The Court concludes as a matter of law that, if files with hash values known to be associated with child pornography are reported to be on the "shared" folder of a suspect's computer, probable cause exists for searching such suspect's computer. Because hash values are analogous to fingerprints and provide high confidence that the contents of files associated with such hash values are known, the images or videos need not themselves be downloaded from the suspect's computer in advance of the issuance or execution of a search warrant. Thus, any question concerning whether, in this case, RoundUp eMule actually effected a single-source download from defendant's computer does not affect the validity of the search warrant.*

United States v. Noden, 2017 WL 1406377 (D.Neb., 2017)

Using Grid Cop software, investigator applied for search warrant of defendant's home. Investigator compared hash values of files advertised by suspect to a CP library of known child pornography. His affidavit, however, falsely stated that he did a browse and direct download from the suspect. The appellate court ruled that it was not a Franks violation because the affidavit supported probable cause after redacting the false information.

The court rejected defendant's argument that Grid Cop was basically an unreliable anonymous tip. In so ruling, the court stated,

> *Grid Cop is a known source that operates with known computer software susceptible to ascertainable statistics regarding accuracy. Its basis of knowledge is clearly demonstrated and its veracity may be readily checked. As such, the warrant affidavit did not rely on an anonymous tip; it contained information from a known source used by specialized law enforcement personnel tasked with investigating child pornography activity*

Ray v. State, 798 S.E.2d 82 (Ga.App., 2017)

Evidence supported finding that the information provided by neighbor, who informed police that defendant regularly used her password protected internet service, was reliable, in sexual exploitation of children action based on file sharing of child pornography where defendant challenged the issuance of search warrants for his house and vehicle; police initially executed a search warrant at neighbor's house based on neighbor having the internet protocol (IP) address associated with the child pornography files, police found no child pornography on the computers and electronic devices at neighbor's house, neighbor was very cooperative with police, and she informed police that defendant sat in his truck in her driveway and used her internet during the time when the child pornography files were shared.

Magistrate had a substantial basis for concluding that probable cause existed for the issuance of search warrants for defendant's residence and truck; the Georgia Bureau of Investigation (GBI) detected child pornography being distributed from defendant's neighbor's internet protocol (IP) address, no evidence of child pornography was located during the search of neighbor's residence, computers, and digital devices, and defendant accessed neighbor's password-protected internet service during the timeframe when the GBI detected the distribution of child pornography through neighbor's IP address.

Commonwealth v. Martinez, 476 Mass. 410 (Mass., 2017)

> Affidavit in support of warrant to search apartment provided probable cause to believe that computers and related items connected to possessing or sharing child pornography would likely be found at that location, though named internet subscriber was not listed as, nor confirmed to be, living in unit, police had no information before search linking defendant to residence, and unauthorized user could have been using unsecured wireless network; affidavit described that state police officer had observed computer associated with particular internet protocol (IP) address sharing child pornography via peer-to-peer network and that internet service provider's records revealed IP address had been assigned to internet subscriber at specific physical address during time when child pornography was shared.

United States v. Morgan, 2016 WL 7009115 (8th Cir. Dec. 1, 2016)

> Time lapse did not render stale information in search warrant in child pornography case, although police did not apply for warrant until 75 days after identifying defendant's IP (internet protocol) address and 51 days after associating it with him; affidavit in support of search warrant established a fair probability of finding evidence on defendant's computers, and affidavit attested that collectors of child pornography tended to retain images and that computer programs that downloaded images "often leave[ ] files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files."

People v. Evensen, 208 Cal. Rptr. 3d 784 (Ct. App. 2016), review filed (Dec. 7, 2016)

> Police officers' information that defendant made child pornography files accessible on a peer-to-peer download network was not too stale to support a search warrant's execution, where defendant had been last seen on the peer-to-peer network four months prior to issuance of the warrant.

United States v. Rusnak, No. CR1500894JGZLCK, 2016 WL 6070087, at *5 (D. Ariz. Sept. 28, 2016), report and recommendation adopted, No. R1500894001TUCJGZLCK, 2016 WL 6024445 (D. Ariz. Oct. 14, 2016)

> The affidavit in this case indicates that SA Daniels, initiating the use of software designed to search a specific P2P network for IP addresses sharing

files depicting child pornography, determined that a computer using a certain IP address was being used to share child pornography files and that eight files depicting child pornography were downloaded from the same IP address that was later determined to be assigned to Defendant Rusnak's single family residence. Because there was a fair probability that evidence of child pornography would be found on computers in Defendant Rusnak's residence, the facts and information in the affidavit, combined with reasonable inferences drawn from those facts and information, support a finding of probable cause.

Note: This opinion has a very good discussion regarding the definition of "probable cause." It has a lot of good language, such as "A fair probability is not a certainty or even a preponderance of the evidence."

State v. Gerard, 790 S.E.2d 592 (N.C. Ct. App. 2016)

Detective's affidavit contained sufficient information for magistrate to determine there was probable cause for the issuance of a warrant to search defendant's computer for child pornography, although affidavit did not include any pictures, where affidavit established how detective identified images as child pornography through SHA1 hash algorithm fingerprint of 17 known child pornography files shared through peer to peer file sharing program with computer at specific IP address identified as assigned to defendant.

Note: Affidavit did not specifically describe the CP images, but only stated that they matched hash values of "known child pornography."

United States v. Dunning, 2015 WL 5999818 (E.D. Ky. Oct. 15, 2015)

Court rejects defendant's contention that hash values are not reliable.

Finally, in his objections to the Report and Recommendation, Dunning claims that the affidavit was deficient because it failed to name the law enforcement database used and the procedure for proper use of the database. [Record No. 45] And he contends that the database was used improperly. However, the name of the database was not necessary to establish probable cause. Further, the name of the database, "The Child Protection System," has now been provided to Dunning along with the manual for its operation that Dunning attached to his motion. Dunning has offered no proof that Detective Merlo abused CPS or violated any procedures required for its use.

U.S. v. Thomas, 788 F.3d 345 (2d Cir. 2015)

Neither the fact that it was private entity which had created computer software used by law enforcement to identify internet protocol (IP) addresses of computers sharing files that were thought to contain child pornography using peer-to-peer program nor commercial name of the software was material information, whose nondisclosure in search warrant affidavit affected validity of search conducted pursuant to warrant issued by magistrate; primary factor that determined whether information obtained by law enforcement using computer software provided probable cause to believe that child pornography would be found on suspect's computer was functionality of software, rather than its creator or name, and functionality of software, along with all material facts relating to law enforcement's reliance thereon, were clearly described in affidavit.

District court did not clearly err in its finding as to reliability of computer software developed to identify what internet protocol (IP) addresses were sharing files thought to contain child pornography using peer-to-peer program, by automatically aggregating publicly available information in manner that could also be accomplished manually by law enforcement, but at slower and less efficient pace; there was nothing in record to suggest that this software reported false or misleading information, and law enforcement, prior to applying for warrant to search home associated with IP address identified by program, verified and corroborated information obtained from program by performing hash-value analysis.

U.S. v. Schumacher, 2015 WL 3424796 (C.A.6 (Ohio))

Governments failure to adequately P2P software did not defeat probable case and did not require Franks hearing.

Government is not required to establish scientific reliability in search warrant affidavit.

Marsh v. U.S., 2015 WL 2450593 (M.D.N.C.)

The fact that P2P software had not undergone independent testing did not defeat probable cause.

U.S. v. Burns, 2015 WL 1746485 (D.Minn.)

*The presence of that one video segment on defendant's computer—in and of itself—provided probable cause for a search of his home. See United States v. Harner, No. 09–CR–0155, 2009 WL 2849139, at *1 (D .Minn. Sept. 1, 2009) (finding probable cause where officer "downloaded and viewed a portion of one file"), aff'd, 628 F.3d 999 (8th Cir.2011).*

> *As to the other files, the investigators matched them to reference files that had previously been viewed and that the affidavit accurately described. The descriptions detailed the contents of the files, including the approximate ages of the individuals portrayed and their actions. This is sufficient to establish probable cause.*
>
> *In short, Sgt. Hanson's estimate of the females' ages, based on his training and experience as an investigator with the ICAC, was sufficient to establish probable cause that the files stored on defendant's computer depicted minors*

U.S. v. Feldman, 2015 WL 248006 (E.D.Wis.) Historical data with known hashes is PC

> *Probable cause is far short of certainty; it requires only a probability or substantial chance of criminal activity, not an actual showing of such activity or even a probability that exceeds 50 percent.*
>
> *The OCE was unable to download the files in this case, but s/he did identify them by hash values. Courts have found hash values sufficiently reliable, even in the absence of a direct download.*
>
> *Relying on his expert, defendant further contends that it may be possible for hash values to be present on a computer without the computer having any significant portion of the file present on it (like having the table of contents of a book without having any of the chapters). But this possibility does not defeat probable cause, which requires only a substantial chance that a search will turn up evidence of criminal activity.*

U.S. v. Gibson, Slip Copy, 2014 WL 6473436 (D.Minn.)

> *"Accordingly, the mere fact that few images or even a single image of child pornography was discovered on the computers will not prevent a finding that Judge Larson had a sufficient basis to conclude that probable cause existed."*

State v. Aguilar, Slip Copy, 2013 WL 6672946 (Tenn.Crim.App.)

> Standard P2P affidavit and warrant established probable cause to search defendant's home.

U.S. v. Schesso, 2013 WL 5227071 (C.A.9 (Wash.))

Allegations that defendant took affirmative step of uploading and distributing a child pornography video on peer-to-peer (P2P) network designed for file sharing and trading provided probable cause for issuance of warrant for electronic search of computer equipment and digital storage devices in defendant's home, for evidence of possession of or dealing in child pornography.

State v. Aston, 2013 WL 4746760, La.App. 5 Cir.,2013.

Information contained in warrant affidavit established probable cause for search of premises at which defendant's computer was located; affidavit set forth that investigating officer located computer used in sharing images of child pornography, compared file listing and corresponding numerical values by which individual images could be identified to list of such values previously identified as child pornography, examined file and confirmed that it was child pornography, located internet protocol (IP) address linked to that computer, and ascertained individual to whom such IP address was assigned, as well as such individual's address.

U.S. v. Dodson, 2013 WL 4400449 (W.D.Tex.) (CPS eDonkey Case)

Warrant affidavit provided substantial basis for concluding that probable cause existed to search defendant's computer for evidence of possession and distribution of child pornography; affidavit detailed the type of software used by Government in the investigation and facts from the ensuing investigation, described the files containing child pornography associated with the IP registered in the name of defendant's son, explained how Government agents located an IP address they eventually traced to defendant's residence, and identified defendant's son leaving the residence and observed a vehicle registered in his name.

U.S. v. Bershchansky, 2013 WL 3816570 (E.D.N.Y.)

Search warrant was supported by probable cause that evidence of possession of child pornography would be found in defendant's apartment; agent's affidavit in support of warrant stated that Homeland Security investigator located files with names known to be associated with child pornography being hosted for peer-to-peer sharing from Internet Protocol (IP) address that was traced to an account holder at defendant's residence, and investigator subsequently downloaded from other sources files with the identical Secure Hash Algorithm Version 1 (SHA1) value, or digital fingerprint, for each of the files identified as indicating child pornography, and confirmed that those files contained graphic child pornography images.

U.S. v. Gozola, 2012 WL 3052911 (D.Minn.)

Peer to Peer investigation supported probable cause for a search warrant.

U.S. v. Chiaradio, 684 F.3d 265 (1st Cir. 2012)

Probable cause supported issuance of search warrant in investigation that led to defendant's prosecution for possession and distribution of child pornography, where supporting affidavit chronicled FBI agent's investigation via enhanced peer–to–peer file–sharing program and how that led to discovery of defendant's internet protocol (IP) address and, in turn, his residence, there was no requirement that program be subjected to scientific peer review to ensure its reliability, and, even if affidavit improperly omitted statements as to program's reliability, those omissions would have increased, rather than decreased, affidavit's persuasive force.

U.S. v. Haymond, 672 F.3d 948 (10th Cir. 2012) (staleness)

Affidavit submitted by Federal Bureau of Investigation (FBI) special agent in support of search warrant was sufficient to establish probable cause to search defendant's home for evidence of child pornography, even though 111 days had elapsed between initial incidents linking defendant to online child pornography and date on which agents submitted affidavit, where affidavit described in detail agent's undercover investigation of peer-to-peer file sharing client program, including fact that he observed user with internet protocol (IP) address linked to defendant's residence who had numerous files of child pornography available for other users to access, view, and download.

U.S. v. Carter, 2012 WL 604162 (W.D.Pa.)

Court ruled that explicit file names seen in peer to peer investigation supported probable cause for a search warrant.

U.S. v. Nolan, 2012 WL 1192183 (E.D.Mo.)

Court ruled there was probable cause for a search warrant based on basic P2P investigation involving direct download.

The court rejected defendant’s argument that a search warrant was needed to download files from defendant’s shared folder.

People v. Deprospero, 91 A.D.3d 39, 932 N.Y.S.2d 789, 2011 N.Y. Slip Op. 08421

“Specifically, the investigator noticed that a certain IP address was a download candidate for suspected pornography files over 40 times in a

period of approximately two weeks, compared three specific files associated with that IP address to files recovered in previous investigations to verify that they depicted child pornography, and traced the IP address to defendant's home. Those facts thus provided the reviewing magistrate with information to support a reasonable belief that defendant possessed child pornography."

State v. Mahan, 2011 WL 4600044 (Ohio App. 8 Dist.)

"McGinnis's affidavit and testimony adequately provided a substantial basis for concluding that the information obtained from Peer Spectre was credible and reliable, including, but not limited to the following: McGinnis has many years of experience investigating internet child pornography. He was aware of Peer Spectre's accuracy based on information he learned from other agencies. He was trained specifically on the use of Peer Spectre and knew that Peer Spectre searches peer-to-peer, or file sharing, networks. McGinnis had used other software programs to search peer-to-peer networks and obtained the same information he got from using Peer Spectre. He has never known the other programs to search beyond shared files."

U.S. v. Beatty, 2011 WL 2728298 C.A.3 (Pa.),2011.

Defendant argued that no one involved in the issuance of the warrant viewed the files, which, combined with the lack of a reasonably specific description of the contents of the files, did not allow the magistrate judge to make an independent assessment of probable cause.

The court ruled,

*Just as we found in Miknevich, the graphic titles of the files found on Beatty's computer "contained highly graphic references to specific sexual acts involving chi ldren." FN1 Id. Additionally, the SHA 1 values belonging to the files on Beatty's computer bore the same SHA 1 values as known child pornography in the Wyoming ICIC Task Force database. Together, these factors allowed a strong inference to be made by the magistrate judge which establishes probable cause. Therefore, the District Court correctly concluded that "the Magistrate Judge was entitled to infer from the highly descriptive and graphic file names and the other information presented in the affidavit [the SHA 1 values] that there was a fair probability that [Beatty?s] computer would contain material prohibited under either 18 U.S.C. §§ 2252 or 2252A." Beatty, 2009 WL 5220643, at * 11.FN2 The motion to suppress was properly denied.*

U.S. v. Gillman, 2011 WL 3288417 C.A.6 (Tenn.),2011 **Unsecured Wireless**

Court rejected defense argument that possibility of another user accessing defendant's unsecured wireless connection defeated probable cause. In rejecting this argument, the court stated,

> *The IP address here established a sufficient nexus connecting the sharing of child pornography to Gillman's residence and computer. Gillman is correct—he could have used a wireless network and someone else could have accessed that network and shared child pornography. This possibility, however, does not negate the fair probability that child pornography emanating from an IP address will be found on a computer at its registered residential address.*

The court also ruled that a 5 month delay between the time child porn was seen at defendant's IP and the time the warrant was obtained did not make the evidence stale.

U.S. v. Miknevich, --- F.3d ----, 2011 WL 692973 C.A.3 (Pa.),2011.

Affidavit in support of search warrant authorizing seizure of defendant's computer contained sufficient facts to support finding of fair probability that defendant possessed child pornography on his computer, so as to provide probable cause for state court judge's issuance of warrant; although affidavit provided no description of substance of images on suspect video file found to be located at IP address corresponding to defendant's computer, the title of the computer file contained highly graphic references to specific sexual acts involving children, referring to the children's ages as six and seven years old, and to graphic sexual activities, and affidavit related that officer who identified the file recognized file's Secured Hash Algorithm value, SHA-1, as one indicating child pornography.

State v. Williams, 35 Fla. L. Weekly D2440a (Fla. 1st DCA 2010):

The trial court suppressed the warrant based upon the detective's failure to provide specific times and dates that the CP images were accessed and based upon the use of the term "suspected child pornography." The appellate court overruled the trial court by using a practical common-sense analysis and looking at the totality of the facts and circumstances. The appellate court also ruled that the good faith exception applied in either case.

Officer's warrant affidavit set forth facts upon which a reasonable magistrate could find probable cause to support issuance of warrant to search defendant's residence for child pornography; five-page supporting

affidavit clearly indicated officer had reason to believe defendant, on at least 123 separate occasions, used a computer in his residence to access a specific IP address and download "known or suspected child pornography," and affidavit also clearly indicated there was at least one occasion where defendant accessed a file that officer personally confirmed contained a video of pre-pubescent females engaging in sexual conduct.

When attempting to secure a valid search warrant, an applicant is not required to provide a magistrate with direct proof the objects of the search are located in the place to be searched, but must rather supply a sworn affidavit setting forth facts upon which a reasonable magistrate could find probable cause to support such a search; the issuing magistrate will then analyze the information contained in the affidavit, consider the type of crime being investigated, examine the nature of the items sought, and make a practical, common-sense decision as to whether there is a fair probability evidence of a crime will be found at a particular place.

In conclusion, the court stated:

> *Here, the Defendant was suspected of possessing child pornography. A "practical, common-sense" reading of the five-page supporting affidavit clearly indicates Officer Husar had reason to believe the Defendant, on at least 123 separate occasions, used a computer in his residence to access a specific IP address and download "known or suspected child pornography." The affidavit also clearly indicates there was at least one occasion the Defendant accessed a file that Officer Husar personally confirmed contained a video of pre-pubescent females engaging in sexual conduct. Based on the above information, it is reasonable to presume the county judge made a common-sense inference in determining there was a fair probability the Defendant had stored images of child pornography on a computer or other electronic storage device located in his residence…*
>
> *Even if the specific sections of the affidavit where Officer Husar lists the dates the Defendant used his computer to commit illegal conduct, when read in isolation, can be interpreted as vague; a practical, common-sense review of the entire affidavit leaves little doubt the BCSO had probable cause to warrant searching the Defendant's residence for evidence of child pornography.*

U.S. v. Renigar, 613 F.3d 990 (10th Cir. 2010)

Information in search warrant affidavit, which linked the Internet Protocol (IP) address associated with defendant's residential address to child pornography, as well as the affidavit's discussion of computer technology, provided an adequate nexus between the alleged crime and the location to be searched to cause a person of reasonable caution to believe that evidence of the possession and/or transmission of child pornography would be found at that residence.

Discussion: There was a direct download by FBI agents on this case.

U.S. v. Henderson, 595 F.3d 1198 (10th Cir. 2010):

Affidavit failed to establish probable case because affiant did not adequately explain how information was collected by WTK. Good faith exception applied.

Relevant excerpts follow:

His affidavit, however, does not identify: (1) who informed Leazenby that a computer with the relevant IP address had transferred child pornography; or (2) the method used in this case to establish that a computer at the specified IP address transferred videos with child-pornography-associated SHA values.

Nevertheless, the court determined "the reliability of the information [is], in this case, insufficient to establish probable cause" because Leazenby's affidavit did not indicate the source of the listed IP address and SHA values

The government wisely conceded at oral argument that Leazenby's affidavit is insufficient to establish probable cause. Notably, the affidavit fails to identify how Leazenby's source determined that a computer with the relevant IP address-rather than some other computer-shared videos with child-pornography-related SHA values.FN4

FN4. Although the district court determined that "[t]he science behind 'fingerprinting' ... these computers appears rock solid," it apparently overlooked the fact that the affidavit does not state that Leazenby's source in fact engaged in the scientific, rock-solid method generally used by law enforcement.

State v. Nuss, 279 Neb. 648, 781 N.W.2d 60 (Neb. 2010)

Affidavit was insufficient to establish probable cause for issuance of warrant to search defendant's residence for evidence of visual depiction of sexually explicit conduct involving minors, where actual downloaded images intercepted during undercover investigation did not accompany the affidavit, affidavit did not use or even refer to the statutory definitions of sexually explicit conduct in describing the intercepted images relied upon as probable cause for the requested search warrant, but instead referred to filenames "which are consistent with child pornography" and images which "appear to be child pornography" without stating the actual filenames or describing the particular conduct depicted in the images, and applicable state criminal statutes, unlike their federal counterparts, did not include a definition of "child pornography."

Discussion: This was an FBI peer to peer case.

U.S. v. Beatty, 2009 WL 5220643 (W.D.Pa.) **PC based on file names and labels**

Officers applying for peer-to-peer search warrant affidavit never actually viewed nor described the images in question, but relied on file names of 11 files and the fact that the Wyoming ICAC Taskforce designation the SHA1 values as "known child pornography." Court ruled that file names supported probable cause and that the court could use common sense to infer that the designations by WTK were accurate.

U.S. v. Massey, 2009 WL 3762322 (E.D.Mo.): **Unsecured Wireless**

Possibility of someone using Defendant's unprotected wireless signal does not defeat probable cause.

U.S. v. Wellman, 2009 WL 37184 (S.D.W.Va.): **reliance on WTK data**

The officer applying for the search warrant affidavit relied completely on data supplied by WTK. The officer did not view the files personally, but relied on the descriptions of other officers. The court ruled that it was reasonable for the officer to rely on other unnamed officers who are licensed to operate WTK.

U.S. v. Stevahn, 313 Fed.Appx. 138, 2009 WL 405847 (C.A.10 (Wyo.) **failure to establish reliability of software used**

Affidavit lacked sufficient evidence to provide probable cause to issue search warrant to seize defendant's home computer, which was alleged to have been targeted by law enforcement officers from around the world as a download candidate for child pornography; investigating officer's affidavit failed to provide any information as to the investigative techniques other

officers used, the software those officers used or its reliability, or even the identity of the officers or where they were from, and affidavit did not connect investigating officer's experience to observation of other officers.

Investigating officer's reliance on invalid search warrant was not objectively unreasonable, and thus evidence of child pornography seized from defendant's home computer was subject to good faith exception to exclusionary rule; while officer's affidavit was in part boilerplate, it included detailed accounting of various techniques officer used and set forth reason for his belief that search of defendant's home would yield evidence of child pornography, such that a neutral magistrate could independently determine probable cause.

State v. Garbaccio, 214 P.3d 168 (2009): **staleness**

"In this case, it was reasonable for the issuing judge to infer that, based on Detective Bergmann's supporting affidavit, Garbaccio was probably involved in criminal activity and that evidence of the crime of possession of child pornography would likely be found at his residence. The affidavit established that Detective Bergmann had located a known video of child pornography publicly available for download from the IP address assigned to Garbaccio. The titles of 21 other files available for download strongly suggested that Garbaccio collected and was in possession of child pornography. That Detective Bergmann waited five months to apply for a search warrant after he initially investigated Garbaccio's computer use did not eliminate the probative value of this evidence at the time the application was made. Detective Bergmann stated in his affidavit that, based on his training and experience, collectors of child pornography often retain the contraband. Although Detective Bergmann employed boilerplate language in making this statement, the statement provided a sufficient basis for the issuing judge to infer that Garbaccio likely still possessed the images, even five months after Detective Bergmann initiated the investigation."

Discussion: This case discusses how the common extension of staleness rules applies to peer-to-peer cases. Although not discussed in the opinion, the problem with doing a peer-to-peer search warrant five months after observing child pornography in a shared folder is that we do not know who was using the computer at the time the child porn was observed. If we do not know who was using the computer, it would be difficult to rely on the assertion that collectors of child pornography rarely dispose of their images. The government would have to speculate that the person collecting the child porn is still residing at the residence.

U.S. v. Schmidt, 2009 WL 2836460 (E.D.Mo.)) **SHA1 values**

> "Defendant first argues that it is possible that Sergeant Kavanaugh could have made an error when comparing the 32-character SHA1 FN5 value of the video on Defendant's computer to the 32-character SHA1 value of the video known by police to contain child pornography. While Sergeant Kavanaugh may have admitted that he would not have known if he transposed a number, the Court agrees with Magistrate Judge Noce that no evidence adduced at the hearing indicated that the two 32-character SHA1 values were not actually the same. Moreover, human error is always a possibility and is not a legitimate reason to discredit a search warrant."
>
> "In this case, Detective McCartney submitted a sworn, written affidavit in support of his application for the search warrant. This affidavit established that the police had obtained a list of IP addresses that were offering a video file that was known to include child pornography (based on the video's SHA1 value). The officers were then able to determine that one of the IP addresses was used by Joseph Schmidt at 7611 River Walk Place, St. Louis, Missouri 63129. The affidavit also established the efforts of Detective McCartney to verify that the video did include child pornography and that Joseph Schmidt resided at the River Walk Place address. Additionally, the affidavit explained that Detective McCartney knew from training and experience that persons who collect child pornography tend to keep the images for long periods of time for personal gratification and also transfer them to other digital devices. Based on the foregoing, the Court finds that the issuing judge had a substantial basis for concluding that there was a fair probability that contraband or evidence of a crime would be found at 7611 River Walk Place and, therefore, that probable cause existed for the issuance of the warrant."
>
> "Additionally, it is irrelevant that only a single item of child pornography was associated with Defendant's computer at the time that the search warrant was issued… Moreover, in this case, considering the nature of child pornography and those who collect it, the presence of one file on a computer established a fair probability that more files would be discovered."

U.S. v. Cartier, 543 F.3d 442 (8th Cir. 2008): **PC based on hash values and PC based on reliability of referrals**

> Probable cause supported search warrant for defendant's computer, although no one reported seeing images of child pornography on defendant's computer prior to execution of the search warrant, the FBI had reliable information from a Spanish law enforcement agency that defendant's computer contained files with hash values matching known child pornography images.

The court rejected defendant's argument that the government did not establish the reliability of the Spanish law enforcement agency after hearing testimony that the FBI considered the Spanish agency a reliable source.

"In arguing that the hash values do not establish probable cause for a search warrant, Cartier asserts that it is possible for two digital files to have hash values that collide or overlap… Cartier's expert testified that hash values could collide and that in laboratory settings these values had done just that. However, the government's expert witness testified that no two dissimilar files will have the same hash value." The court sided with the government.

Warrant was not defective for failing to include a search strategy.

U.S. v. Cartier, 2007 WL 319648 (D.N.D.)): **PC based on hash values**

Government obtained a search warrant based solely upon hash values placed into peer to peer program and documenting which IP addressees were sharing that hash. Cartier argued no probable cause existed for the search warrant because only the hash values were used to establish probable cause. After hearing experts from both sides regarding the reliability of hash values, the court overruled the motion to suppress.

U.S. v. Massey, 2009 WL 3762322 (E.D.Mo.):

"This Court finds that, even accepting the assertion that the IP address could have been hijacked by a third party, the Affidavit provided probable cause to find that evidence of child pornography would be at 7378 Hazel Avenue."

Discussion: The opinion cites several other federal opinions that have ruled that tracing an IP address to the suspect's house is sufficient for probable cause, even if it was possible that someone else was accessing the IP address.

U.S. v. Bradley, 2010 WL 2471885 (E.D.Ky.) **PC based on GUID**

Peer to Peer investigation showed that child porn was seen at an IP address assigned to a fire station. Officer asked Bradley if he could look at his Limewire.props file. After receiving consent, officer saw that GUID in Limewire.props file matched the GUID from the peer-to-peer records. Officer seized computer and got a search warrant 26 hours later. Court ruled that matching GUID provided probable cause to believe this was the correct computer. Threat of destruction of evidence provided exigent circumstances to seize it. 26 hour delay in obtaining warrant did not render seizure unreasonable.

Discovery Issues:

United States v. Harper, 2023 WL 4746764 (C.A.6 (Tenn.), 2023)

Defendant requested a copy of Torrential Downpour program. The appellate court ruled the trial court was correct in denying discover request. The court noted, "when the request seeks information cloaked in law enforcement privilege, we must weigh the competing interests of a defendant's articulated needs in receiving that information with the government's desire to protect it from disclosure." The court then said the defense did not present any evidence of government wrongdoing. The defendant's claim that he needed to verify the program works as the government testified is insufficient.

United States v. Owens, 18 F.4th 928 (C.A.7 (Wis.), 2021)

In general, a defendant will not be able to make a prima facie case that disclosure of the government's confidential software is material to his defense, as required to support a motion to compel discovery of the software, if he cannot present a cogent defense theory, supported by some facts, for which discovery relating to the software would help develop.

A defendant may fail to make a prima facie showing that disclosure of the government's confidential software is material to his defense, as the basis for denying a motion to compel discovery of the software, if the government presents evidence based on information produced to the defendant that fatally undermines the proffered theory.

Defendant was not prejudiced by denial of motion to compel discovery of government's confidential software program used to participate in, detect and download child pornography from peer-to-peer shared folders, its source code, and all supporting documents, in trial for distribution of child pornography, even though agents who executed search of his computer were unable to locate particular video file that had been downloaded twice and formed basis of charge, where testimony of government's expert that video file had been opened in defendant's file-sharing network account while government's investigation was occurring, and that file with same filename as target video was present in defendant's "most recently used" folder, undermined defendant's concern regarding risk that software created "false positive" as to existence of video on his computer.

United States v. Thomas, 2021 WL 3857768, at *1 (M.D.Fla., 2021)

Defendant moved to compel production of P2P software, arguing it might be searching beyond the shared folder or doing other assorted nefarious things. The court denied the motion, ruling materiality was not shown. The court made note that the government was only going forward on the images found on the suspect's computer.

United States v. Duggar, 2021 WL 3699864, at *1 (W.D.Ark., 2021)

The government provided the defendant with a screenshot of the Roundup Bittorrent screen in discovery. The defendant filed a motion to compel production of the data in other tabs that could be seen on the screen. The government convinced the court that none of that data was material to the case, so the motion was denied.

United States v. Shipton, 5 F.4th 933 (C.A.8 (Minn.), 2021)

In prosecution of defendant for possessing child pornography, speculation by defendant as to the possibly faulty nature of programs used by police officer to identify and download part of a file from peer-to-peer file-sharing network, a file that was later verified to contain child pornography and to originate from an internet protocol (IP) address associated with defendant, was insufficient basis for district court to be under any compulsion to order independent testing of the programs to ensure that they were reliable and did not access private spaces on defendant's computer; defendant, in requesting such testing, was essentially seeking authorization for a fishing expedition.

United States v. Clarke, 979 F.3d 82 (C.A.2 (N.Y.), 2020)

Defendant charged with child pornography offenses failed to show that he was prejudiced by limitation imposed by district court on his discovery of software developed for law enforcement to identify individuals sharing files known to contain images of child pornography using peer-to-peer file-sharing network, and software's source code; while defendant and his expert asserted that child pornography files stored on defendant's computer were not publicly available on file-sharing network since they were stored on an external hard drive, government demonstrated that network's software had an option that permitted defendant to designate location for storage of files.

United States v. Gonzales, 2020 WL 5210821 (D.Ariz., 2020)

Defendant was charged with distribution of child pornography based on a Torrential Downpour BitTorrent investigation. Since no child pornography was found on suspect's computer and the government relied on the software to prove their distribution charge, the court allowed defense experts to conduct independent testing at a government facility. The defense experts were Tammy Loehrs and her partner, Michelle Bush. The court refused to allow the experts to obtain their own copies of the software and refused to let them access the COPS database. The opinion gives a detailed discussion of each of the tests performed by the experts and notes that all of them show the program works just as the government says it does. This case is a good resource to use when defense makes such requests. Some of the court's findings regarding the tests conducted are as follows:

- *This demonstrated that Torrential Downpour does not download a file from a suspect computer once the file has been deleted.*
- *This demonstrated that Torrential Downpour does not download a file that has been moved from the shared folder on the suspect computer.*
- *Torrential Downpour did not obtain the files from the deleted or non-shared space in any of these tests.*
- *In other words, in each of the tests run by Defendant's experts, Torrential Downpour performed as the government claims: it did not download files that had been deleted or moved to non-shared space.*
- *Tests three and four were designed by Defendant's experts and confirmed in each instance what the government has represented about Torrential Downpour – that it does not somehow enter non-shared space to download files.*
- *The tests thus confirm that if Torrential Downpour downloads files from a suspect computer, it does so because the files are in the shared space, available for download – the act of distribution alleged in this case.*
- *The testing resulted in no obvious failures, meaning Torrential Downpour did not connect to other IP addresses to download data when the data was unavailable on the suspect computer.*
- *The defense testing conducted to date does not cast doubt on the government's representations regarding Torrential Downpour. If anything, it supports those representations.*

United States v. Nguyen, 2020 WL 1812227 (S.D. Cal. Apr. 9, 2020)

Defendant made an ineffective assistance of counsel claim because his attorney failed to obtain CPS software in discovery or at least to try to subpoena it. Court said counsel was not ineffective because he likely would not have been able to obtain it any way. The court reviews other

opinions on the issue and said the defendant likely did not meet the materiality standard.

United States v. Arumugam, 2020 WL 949937, at *4 (W.D. Wash. Feb. 27, 2020)

Defendant filed a motion to suppress alleging Roundup conducted an unlawful search of his computer. He then filed a discovery demand asking for Roundup source code, manual, hash set and other related material. The court denied the request saying defendant did not show materiality of the requested information. Speculating a theory of defense is not enough. Additionally, the court noted,

> *Finally, the Court shares the government's concerns regarding the sensitivity of RoundUp, its source code, hash value and download candidate databases, and related evidence. Dkt. #71 at 23-27; see also Blouin, 2017 WL 2573993, at *3 (quoting United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. 2015)) (agreeing that "granting the defendant's request for the [RoundUp] source code would 'compromise the integrity of [the government's] surveillance system and would frustrate future surveillance efforts"). However, because defendant has not met his burden to establish the materiality of the requested evidence, the Court declines to reach the merits of the government's law enforcement privilege argument.*

United States v. Owens, 2019 WL 6896144 (E.D. Wis. Dec. 18, 2019)

For the reasons set forth above, the court finds that Owens has failed to establish that the information sought in his discovery request is material to his defense. The court also finds that the information requested is protected by the law enforcement investigatory privilege and that the public interest in non-disclosure substantially outweighs any interest of the defendant in acquiring it. Owens has failed to show that disclosure of further information related to TDR is either relevant or helpful to the defense.

Defense requested a copy Torrential Downpour BitTorrent software to determine why the file downloaded by law enforcement was not found on his computer and to see if the program searched private areas. The opinion provides a good description on how the program works and summarizes the testimony pertinent to the issues.

United States v. Hoeffener, 2020 WL 873369 (8th Cir. Feb. 24, 2020)

District court did not abuse its discretion in child pornography prosecution in denying defendant's motion to compel government to produce source code, manuals, and software used to identify individuals offering to share or possess files known to law enforcement to contain images or videos of child pornography, despite defendant's contentions that government's software might possibly have accessed non-public areas of his computer or that there was possibility that it malfunctioned, where government disclosed information that allowed defendant's expert to investigate how file sharing software that defendant was using functioned, how government's software functioned, and activity log gathered from defendant's computer. (Torrential Downpour)

State v. Lovell, 2019 WL 2031011, (Wis.App., 2019)

Trial court denied defendant's request to conduct forensic examination of Detective's computer. Defendant argued that it was possible that the Roundup program searched defendant's computer outside of the sheared folder. Appellate court ruled that defendant did not have a right to forensically examine the detective's computer. First, the court ruled that mere speculation is insufficient to warrant such a thing. Second, the court ruled that since the government was prosecuting solely on the evidence found during the search warrant execution and had no intention to introduce any Roundup material at trial the evidence was not material to the case.

United States v. Gonzales, 2019 WL 4040531, at *1 (D.Ariz., 2019)

In a follow-up to the previous case listed below, the court addresses 9 separate tests the defense expert (Loehrs) wants to conduct on the Torrential Downpour software. The opinion provides an exhaustive discussion as to how the system works and explains why she can run some of the tests, but not others. Her desire to access their database was one of the biggest points of contention.

United States v. Gonzales, 2019 WL 669813, at *6 (D.Ariz., 2019)

Because Gonzales has shown that the Torrential Downpour is material to his defense, he should be given access to the program to investigate its reliability and help him prepare for cross-examination of Agent Daniels.

Defendant sought an installable copy of the software and associated training and user manuals. He did not ask for source code. The defense presented an affidavit and from expert Tami Loehrs wherein she stated that the downloaded files were not found on defendant's device. She went on to explain how most software contains bugs and flaws and that the files downloaded may have been from other users. The court ruled that her testimony was sufficient to establish materiality.

The court rejected defendant's contention that a 4th Amendment violation occurred. The defendant claimed "Torrential Downpour is material to a Fourth Amendment challenge because the program "searches beyond the public domain, essentially hacks computers searching for suspect hash values, and therefore conducts a warrantless search." The court ruled that there was no evidence to support the materiality of this claim.

After finding the defendant met the materiality standard, the court addressed the government's argument that the program was subject to the law enforcement privilege. The court did a balancing test and ruled that the government's need to keep the program protected outweighed the defendant's need to have a copy. In a compromise, the court said the defendant could examine the software at a government facility, but could not make any copies.

In a companion case, Ordonez, the court ruled that no materiality was shown and denied defendant's request.

The court denied defendant's argument that the software met the Brady standard.

This opinion gives a good review of the various courts that have ruled on the same issue.

United States v. Alva, 2017 WL 6820149 (D.Nev., 2017)

In denying defense's request to view the source code of Roundup software, the court concludes,

> *Defendant does not dispute that the RoundUp software downloads only from a single source. Further, he submits generalized contentions with no evidence that RoundUp somehow searched his entire computer. He does not present evidence or even allege, as the defendant in Budziak did, that the P2P program used in the instant case allows a user (or a connecting "peer," e.g., a law enforcement agent) to modify the sharing settings. Instead, Defendant relies upon*

> *possibilities and conjecture. Defendant's request fails to meet "the requirement of specific facts, beyond allegations, relating to materiality.*

United States v. Blouin, 2017 WL 3485736, at *7 (W.D.Wash., 2017)

> *The Court remains persuaded that defendant does not need the source code to mount his defense. As indicated in the Order denying defendant's motion to compel, unlike the defendant in Budziak, defendant here does not contend that the program at issue allows law enforcement to modify the sharing settings on target computers. Instead, he challenges the reliability of the single-source downloading feature of RoundUp eMule.*

United States v. Hoeffener, 2017 WL 3676141 (E.D.Mo., 2017)

> Defendant was not entitled to user manuals and source code of Torrential Downpour software in discovery. Defendant had not sufficiently demonstrated that the requested information is material to Defendant's defense and the requested information is protected from disclosure as a sensitive law enforcement investigation technique.

State of Ohio v. Wilkie, 2017 WL 1436370 (Ohio App. 3 Dist., 2017)

> Court properly denied defendant's request for a copy of government's ShareazaLE software. Defendant offered no evidence to support theory that software searched files outside the shared folder.
>
> Court also ruled for government on *Franks* hearing issue and suppression issue.

U.S. v. Pirosco, 787 F.3d 358 (6th Cir. 2015)

> The District Court did not abuse its discretion in denying the motion of a defendant, who was charged with knowingly receiving and distributing child pornography and knowingly possessing child pornography, to compel production of a proprietary program that law enforcement used to download files from defendant's computer, despite claim that the software could give law enforcement officials the ability to manipulate settings or data on the target computer, even unintentionally, where there was no evidence that the government illegitimately obtained child pornography from defendant's shared folders.

The District Court did not abuse its discretion in denying the motion of a defendant, who was charged with knowingly receiving and distributing child pornography and knowingly possessing child pornography, under a statute that set for the offense and receipt or distribution, to compel production of a proprietary software program that law enforcement used to download files from defendant's computer; defendant did not contest that he received child pornography, and, even if it were necessary, he had admitted to facts that would make the software program immaterial.

Requests for discovery fall outside the scope of the materiality provision of the rule governing discovery if a defendant is not seeking the discovery to aid in the preparation of his defense, but is attempting to obtain the discovery for the purpose of gathering materials to support various sentencing arguments.

State v. Roberts, 2015 WL 404627 (Utah):

Trial court did not abuse its discretion in denying defendant's motion to compel discovery of law enforcement's computer database of digital file values corresponding to files containing child pornography and software that searched peer-to-peer file sharing network for identified values, to extent that motion included methodologies and all values in database, in prosecution for sexual exploitation of a minor arising from child pornography on defendant's computer; such discovery would not likely produce evidence defendant sought, which was verification that files defendant had shared and that database had detected were indeed child pornography, since government relied on officer's review of files, rather than database's values, to verify that files contained child pornography.

U.S. v. Feldman, 2015 WL 248006 (E.D.Wis.)

The magistrate judge denied defendant's motion to compel disclosure of the RoundUp program, its manual and protocols, and its technical specifications, concluding that defendant failed to show that this information was "material to preparing the defense." Fed.R.Crim.P. 16(a)(1)(E). The magistrate judge noted that while the government used RoundUp to identify defendant as a suspect, the receipt/possession charges against him are based on the evidence recovered from his home pursuant to the search warrant.

U.S. v. Dillow, 2013 WL 5863024 (N.D.Ohio)

As a matter of first impression, in prosecution of defendant for receipt, distribution, and possession of child pornography, that local law enforcement had the computer software used to establish defendant's possession of child pornography did not mean that federal prosecuting

attorneys had possession of the software, or that they were obligated to obtain it, such that defendant was not entitled under the rule governing discovery in criminal proceedings to identification of, or an opportunity to inspect, the software.

U.S. v. Brashear**,** Slip Copy, 2013 WL 6065326 (M.D.Pa.)

Defendant issued a subpoena duces tecum to Pennsylvania State Police asking for source code of the Roundup program. Defense counsel argued that he needed to see the source code to determine if there were any violations of the Fourth Amendment, ECPA, Wiretap Laws or the Gnutella Protocol. The court ruled that the source code is not relevant to any of these issues and quashed the subpoena.

"The investigation of a file sharing program does not involve any physical trespass onto a constitutionally protected area. Trooper Powell did not physically enter Brashear's home or access his computer. Instead, Trooper Powell simply used a program that identified child pornography available on a public ***peer-to-peer*** *file sharing program. This investigation involves "the transmission of electronic signals without trespass" and does not implicate Brashear's Fourth Amendment rights under Jones."*

U.S. v. Budziak, 697 F.3d 1105 (9th Cir. 2012)

Defendant charged with distribution of child pornography should have been granted discovery as to the software application used by the Government to discover incriminating evidence; defendant presented evidence suggesting that the Federal Bureau of Investigation (FBI) may have only downloaded fragments of child pornography files from his "incomplete" folder, making it "more likely" that he did not knowingly distribute any complete child pornography files to agents, and he submitted evidence suggesting that the FBI agents could have used the software to override his sharing settings.

Neither a general description of the information sought nor conclusory allegations of materiality suffice to entitle a criminal defendant to discovery, but rather, a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.

Where a defendant seeking discovery from the government has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless; criminal

defendants should not have to rely solely on the government's word that further discovery is unnecessary.

Case was remanded to determine whether source code would have affected verdict, but the government lost the source code and could not produce it. See 2015 WL 2242152 (C.A.9 (Cal.))

U.S. v. Chiaradio, 684 F.3d 265 (1st Cir. 2012)

Defendant was not entitled to compel production of source code of enhanced peer–to–peer file–sharing program utilized by FBI in investigation that led to defendant's prosecution for possession and distribution of child pornography, under rule regarding disclosure of evidence material to preparing defense or that government planned to use in its case in chief, where defendant was not prejudiced by non–disclosure, as government gave defendant digital file recording transfer from defendant's laptop computer to agent's computer and copy of FBI guide detailing how to reconstruct program session manually, and presented evidentiary hearing testimony that agents had used those materials to reconstruct transfer to verify its origin on defendant's computer.

Lack of peer review in scientific community was not determinative on district court's *Daubert* determination as to whether to allow proposed expert testimony regarding reliability of enhanced peer–to–peer file–sharing program utilized by FBI in investigation that led to defendant's prosecution for possession and distribution of child pornography; that FBI kept source code for program purposely secret, due to reasonable fears that traders of child pornography, as notoriously computer–literate group, would otherwise be able to use source code to develop ways to evade apprehension or to mislead authorities, provided reasonable explanation for lack of peer review.

State v. Mahan, 2011 WL 4600044 (Ohio App. 8 Dist.)

Court properly denied defense counsel's motion to obtain copy of Peer Spectre program and accompanying documents.

This case has a good discussion concerning the reasons why the requested information would not be helpful to the defense.

U.S. v. Budziak, 2009 WL 1392197 (N.D.Cal.)): (reversed by Circuit Court)

Defendant, who was charged with distribution of child pornography, requested a copy of the FBI's proprietary version of LimeWire. Defendant

says that there is a possibility that images on defendant's computer were reassembled from different sources and maintains that the only way he can confirm this is to have their expert conduct an examination of the FBI's enhanced LimeWire program. In denying the motion, the court stated, "[T]his court is unpersuaded as to why confirming that information is necessary or material to defending against the allegation that defendant distributed images from his computer to the FBI some six weeks before."

Wiretap Issues:

Chavis v. State, 2011 WL 3807747 (Tex.App.-El Paso)

Police officer did not "intercept" computer files involving child pornography on defendant's computer, within meaning of the statute making it a crime to intentionally intercept an electronic communication; by using publicly available software to view files defendant made available in shared folder on defendant's computer, the files were not "in flight" at the time officer acquired them.

U.S. v. Willard, 2010 WL 3784944 (E.D.Va.,2010.)

"The Court finds that the use of Peer Spectre did not constitute a wiretap because the software does not intercept electronic communications. The functions performed by Peer Spectre and Wyoming Toolkit are more akin to mining data."

Expert Witness Testimony:

United States v. Carme, 2020 WL 3270877 (D.Mass., 2020)

Defendant argued that the sophisticated nature of the Roundup BitTorrent program violated his privacy rights contrary to the recent Supreme Court cases, such as Carpenter and Jones. The appellate court rejected his argument, but provides a good discussion on the development of the law in that area.

United States v. Shipton, 2019 WL 5330928 (Minn. 2019) *slip copy*

This very thorough case discusses the Roundup and CPS systems in great detail. The court specifically rejected defense expert Loehr's testimony that the programs search outside the shared folders. The court also found her testimony lacked credibility. The court rejected defense arguments that Carpenter and Jones have created an expectation of privacy when the government uses technology to amass great amount of surveillance.

State v. Morrill, 2019 WL 3765586, (N.M.App., 2019) *unpublished*

Trial court did not err in ruling Roundup BitTorrent program was reliable under Daubert standard, even though it was not subject to peer review.

Note: This case contains a good discussion regarding the witnesses the State called in their Daubert hearing and the reliability testimony given.

United States v. Blouin, 2017 WL 3485736, at *6 (W.D.Wash., 2017)

With regard to Ledgerwood, who would be a fact or lay witness with respect to his use of RoundUp eMule, neither Daubert nor Kumho apply. Ledgerwood will be permitted to testify about how he interfaced with the RoundUp eMule program and what resulted from his efforts. Ledgerwood does not have to know about or explain how the program executes its source code; he just has to describe the manner in which he used it

As to Lynn, defendant cannot seriously challenge his expertise or his ability to testify about how he created the program, what the program is designed to do, and whether, in his opinion, the program does what was intended. Computer programming is not a scientific theory or technique, it is not new or novel, and it does not implicate the Court's responsibility to keep "junk science" out of the courtroom. Any doubts about whether RoundUp eMule operates in the manner that Lynn represents go to the weight, and not the admissibility, of his testimony.

With respect to Detective Robert Erdely, who seems to be a fact witness, rather than an expert witness, defendant's motion to exclude also lacks merit. Erdely is proffered by the Government to describe the process for training law enforcement personnel to use RoundUp eMule and to discuss the tests he has performed both as part of the training curriculum and during the course of this case. Erdely need not be a software engineer or have training in computer programming to testify about how a user interfaces with RoundUp eMule and the types of results that can be obtained.

United States v. Maurek, No. CR-15-129-D, 2015 WL 5472504, at *4 (W.D. Okla. Sept. 16, 2015)

P2P search warrants are not subject to Daubert analysis.

U.S. v. Thomas, 2013 WL 6000484 (D.Vt.)

This opinion provides a detailed description of how CPS works and the court destroys the credibility of defense expert Tammy Loehrs. Countless challenges to the CPS system are discredited by the court.

The court rejected the defense expert, by stating, *"On balance, Ms. Loehrs provided little, if any, credible or reliable testimony to support her expert opinions in this case. Accordingly, the court does not rely on her opinions in reaching its conclusions."* The court went into detail about several of Ms. Loehrs' misrepresentations.

U.S. v. Pirosko, Slip Copy, 2013 WL 5595224 (N.D.Ohio) *affirmed* U.S. v. Pirosco, 787 F.3d 358 (6th Cir. 2015)

"There is no precedent or authority demanding that the *Daubert* reliability standard must be applied to investigative procedures used by law enforcement in order for the search warrant to contain probable cause for the search, nor does *Daubert* hold that this standard must be applied to the probable cause analysis. Therefore the Court rejects this argument. Here, the affidavit in question included a sworn statement by the affiant that the investigative procedure used was reliable, as determined by many previous investigations employing this same procedure."

U.S. v. Chiaradio, 684 F.3d 265 (1st Cir. 2012)

Lack of peer review in scientific community was not determinative on district court's *Daubert* determination as to whether to allow proposed expert testimony regarding reliability of enhanced peer–to–peer file–sharing program utilized by FBI in investigation that led to defendant's prosecution for possession and distribution of child pornography; that FBI kept source code for program purposely secret, due to reasonable fears that traders of child pornography, as notoriously computer–literate group, would otherwise be able to use source code to develop ways to evade apprehension or to mislead authorities, provided reasonable explanation for lack of peer review.

Probable cause supported issuance of search warrant in investigation that led to defendant's prosecution for possession and distribution of child pornography, where supporting affidavit chronicled FBI agent's investigation via enhanced peer–to–peer file–sharing program and how that led to discovery of defendant's internet protocol (IP) address and, in turn, his residence, there was no requirement that program be subjected to scientific peer review to ensure its reliability, and, even if affidavit

improperly omitted statements as to program's reliability, those omissions would have increased, rather than decreased, affidavit's persuasive force.

Umg Recordings, Inc. v. Linder, 531 F.Supp.2d 453 (E.D. NY 2007)

Expert's theory of how person used Internet anonymously to infringe copyrights of record companies was sufficiently reliable to be admitted in copyright infringement lawsuit, where opinion was based on objective data provided by peer to peer website investigator and Internet service provider which did not require interpretation or conjecture and expert drew from his experience using that data.

Witness could testify as expert based on his experience as to how file-sharing worked, how it could be used to infringe copyrights, and how seemingly anonymous Internet activity could be linked to user, since virtually no subjective analysis was required and others in field, conducting similar analysis, would have proceeded in same way, and there was no other, more reliable method to do so; although meth-od did not comport with four non-exclusive Daubert factors, Daubert factors were intended as suggestions and were not appropriate for every type of expert testimony.

Other Issues

United States v. Juhic, 954 F.3d 1084 (8th Cir. 2020)

Notations on computer-generated reports created based on agent's computer's interactions with internet protocol (IP) addresses registered to defendant, which identified whether files accessed by agent were “child-notable” or part of a series of child pornography that had been submitted to the National Center for Missing and Exploited Children (NCMEC), were out-of-court statements offered for the truth of the matter asserted, namely that videos and images were child pornography, and thus, the notations were hearsay; it was only after a human determined that a file contained child pornography that the hash value or series information was inserted into the computer program and automatically noted in future reports.

United States v. Fletcher, 946 F.3d 402 (8th Cir. 2019)

Evidence was sufficient for reasonable jury to find defendant guilty of knowing distribution of child pornography, where law enforcement officer testimony described peer-to-peer file-sharing program, including how it allowed user to limit access to files, defendant admitted that he knowingly downloaded and used that program at least for one-way file sharing, evidence indicated that many other persons as well as defendant had in fact

downloaded child pornography from defendant's download-shared folder, and defendant's trial testimony varied substantially from his recorded interview with law enforcement officer where he admitted knowing program included child pornography and resumed doing so after learning the downloads included child pornography images, and repeatedly, out of guilt, deleting those files.

People v. Conner, 2019 WL 4743882, (Cal.App. 6 Dist., 2019) *unpublished*

Defendant objected to use of CPS spreadsheet in P2P prosecution and appellate court ruled it was inadmissible hearsay.

Though it appears much of the information on the spreadsheet was machine-generated and therefore not hearsay, the People's argument does not address the "child notable" designations. Unlike the other information on the spreadsheet, the child notable designations involved human input.

Without any independent verification that the child notable designations on the Child Rescue Coalition spreadsheet actually correspond to child pornography, the trial court erred in admitting the spreadsheet under the business records exception.

We therefore conclude that admitting the evidence violated defendant's right to confront the witness or witnesses responsible for assigning the child notable designations. We note, however, that our opinion should not be construed as forbidding the use of evidence such as the Child Rescue Coalition spreadsheet, with appropriate attention to the confrontation issues discussed here. (Crawford v. Washington issue)

United States v. Dillingham, 2018 WL 2417006 (E.D.Va., 2018)

Defendant could not be convicted of distribution or receipt of child pornography based on files in his shared folder unless government had direct evidence that the defendant had knowledge of the content of the specific images charges and the time of receipt or distribution. Evidence such as search terms and web history were improper propensity evidence. Just because he had an interest in child pornography does not mean he knew the specific content of the files in question.

State v. Yates, 2017-0654 La.App. 1 Cir. 11/1/17, 8, 2017 WL 4969453 (La.App. 1 Cir., 2017) *unpublished*

The defendant argued that he must have accidently downloaded child pornography when seeking adult pornography. He denied ever viewing the images or their file names. The opinion discusses how the forensic

examiners used things like search terms and recently opened file lists to adequately establish intent.

State v. McNitt, 2017 WL 3379191 (Minn.App., 2017)

Defendant asserted that law enforcement used technology "not commonly accessible to the public" to learn the IP address of the computer sharing the suspected child pornography files, and such a search was prohibited by the United States Supreme Court's decision in *Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 2046 (2001). The court rejected this argument, stating that the suspect's IP address was accessible to anyone.

State v. Adamo, 2017 WL 4564568 (N.M.App., 2017)

Detectives executed P2P search warrant and only found deleted images carved from an external hard drive. The court ruled that suspect's extensive P2P activity and the direct downloads of the detectives were sufficient to establish that he knowingly possessed child pornography at some point of time.

United States v. Bates, 2016 WL 6958146 (C.A.11 (Fla.), 2016)

Child pornography investigation reports of Internet Crimes Against Children, Child Online Protective Services (ICACCOPS) and Child Protective System (CPS) were inadmissible hearsay, in prosecution for knowing receipt of child pornography, knowing distribution of child pornography, and knowing possession of computer containing child pornography; reports did not fall into hearsay exception for records of regularly conducted activity because reports required human input, data in reports that matched defendant's downloaded files to known child pornography relied on input from law enforcement officers, and reports included officers' opinions about whether files were known child pornography.

Admission of child pornography investigation reports of Internet Crimes Against Children, Child Online Protective Services (ICACCOPS) and Child Protective System (CPS) violated Confrontation Clause, in prosecution for knowing receipt of child pornography, knowing distribution of child pornography, and knowing possession of computer containing child pornography; reports and underlying data were testimonial, and government used reports to demonstrate steps of sergeant's investigation and to prove that files defendant downloaded were child pornography.

United States v. Kline, 2015 WL 7018618 (S.D. Cal. Nov. 12, 2015)

Defendant filed a motion to suppress claiming that when CPS captured his IP address it was a Fourth Amendment violation. The court rejected this argument and concluded, "The CPS software provided 'unprotected addressing information' and there was no requirement that the agent obtain a warrant."

United States v. Dreyer, 804 F.3d 1266 (9th Cir. 2015)

Naval Criminal Investigative Service (NCIS) special agent violated the Posse Comitatus Act (PCA)-like restrictions prohibiting direct military involvement in civilian law enforcement activities, in connection with his investigation of the sharing of child pornography; special agent and two other agents initiated statewide operation to search for individuals sharing child pornography online, this audit was not limited to military personnel but monitored all computers within geographic area, special agent's report on the Washington investigation formed basis of state warrant to search defendant's home, execution of that warrant yielded the evidence that led to charges against defendant, special agent's investigation thus pervaded the actions of civilian law enforcement, and special agent testified that he was not engaged in "surveillance" but, instead, conducted "active" investigation, conduct that was expressly prohibited as direct assistance.

Although Naval Criminal Investigative Service (NCIS) special agent violated Posse Comitatus Act (PCA)-like restrictions prohibiting direct military involvement in civilian law enforcement activities in connection with his investigation into online sharing of child pornography, resulting in defendant's conviction for possessing and distributing child pornography, suppression of evidence was not warranted to deter future violations; while facts of case were troubling and unprecedented, violations likely resulted from institutional confusion somewhere in military's command structure about scope and contours of PCA and PCA-like restrictions, rather than intentional disregard of a statutory constraint, government acknowledged the need to conform its investigatory practices to the law and already had taken steps to do so, and so government would be given opportunity to self-correct before court resorted to exclusionary rule.

United States v. Ortega, 2015 WL 6566011 (S.D. Ga. Oct. 30, 2015)

Detective issued Comcast subpoena for period ending June 8. He later used a file noted on June 14 to establish PC for the warrant. The court ruled that in was reasonable to conclude that the same subscriber was still assigned the IP and therefore, no warrant problem.

U.S. v. Figueroa-Lugo, 2015 WL 4385935 (C.A.1 (Puerto Rico),2015.)

Evidence of testimony that, in order to download files from a peer-to-peer file sharing service, the user had to actively click on the file, was sufficient to establish that defendant intentionally sought to download child pornography, as required to support conviction for knowing possession of child pornography.

Evidence that a child pornography image had been accessed from a peer-to-peer file sharing service through use of an internet browser on defendant's computer was sufficient to establish that defendant viewed child pornography that he had downloaded from the file sharing service, as required to support conviction for knowing possession of child pornography.
Evidence of expert testimony was sufficient to establish that "anti-virus" software on defendant's computer could not download child pornography by itself, as required to support conviction of defendant for knowing possession of child pornography.

Evidence of defendant's admission that he downloaded child pornography, and that the child pornography files were saved in folders bearing defendant's name on defendant's computer located in his bedroom, was sufficient to establish that he, rather than some else, downloaded child pornography to his computer, as required to support conviction for knowing possession of child pornography.

U.S. v. Hayes, 2015 WL 2445109 (C.A.4 (W.Va.))

Hayes next asserts a Confrontation Clause challenge to the admission of reports indicating that he was sharing child pornography over a peer-to-peer network. The reports were generated automatically by a computer program, not by a person. "Evidence implicates the Confrontation Clause only if it constitutes a testimonial statement—that is, a statement made with a primary purpose of creating an out-of-court substitute for trial testimony." United States v. Reed, 780 F.3d 260, 269 (4th Cir.2015) *(internal quotation marks omitted). Data generated by a machine, where the only source of the statement is the machine printout and not a person, is not subject to the Confrontation Clause.* United States v. Washington, 498 F.3d 225, 229–30 (4th Cir.2007)*; see also* United States v. Lamons, 532 F.3d 1251, 1264 (11th Cir.2008) *(statements made by machines and not by humans are exempt from purview of*

Confrontation Clause). We conclude that the admission of the challenged reports did not violate the Confrontation Clause.

Crabtree v. Commonwealth, 2014 WL 7240063 (Ky.) Knowing Possession

Evidence supported finding that defendant knowingly possessed videos of child pornography, as required to support conviction for possession of matter portraying a sexual performance by a minor; defendant, using file-sharing program, chose file names clearly indicative of child pornography and clicked on file names to start downloading files onto his computer, videos were found on hard drive of his computer, defendant had to have actually initiated download, and he admitted that he downloaded files from program.

Knight v. State, 2014 WL 7243139 (Fla.App. 1 Dist.): Jurisdiction

Investigation of child pornography in shared computer file accessible over the internet in neighboring city was within city police detective's territorial jurisdiction, even though computer was located in neighboring city, where investigation originated inside detective's territory, at the time of origination detective did not know whether computer was located in her territory, and once it became clear computer was located in neighboring city, detective obtained a search warrant pursuant to a mutual aid agreement with neighboring city's police department.

U.S. v. Dreyer, 2014 WL 4474295 (C.A.9 (Wash.)) Jurisdiction

The broad investigation of a special agent of the Naval Criminal Investigative Service (NCIS) into the sharing of child pornography violated the regulations and policies proscribing direct military enforcement of civilian laws, where the agent searched for sharing of child pornography by anyone within the state of Washington, not just those on a military base or with a reasonable likelihood of a Navy affiliation, and the agent's investigation was not in support of any civilian law enforcement action.