Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	Case No. 3:17-cr-0095 SLG
	)	
vs.	)	
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	
	)	

C-3 MOTION TO COMPEL DISCOVERY AND PRODUCTION OF EVIDENCE: TORRENTIAL DOWNPOUR SOFTWARE

A period of excludable delay under 18 U.S.C.§3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. A total of 36 days remain before trial must commence pursuant to the Speedy Trial Act.

Comes now, Defendant, Matthew Schwier, by and through counsel, Robert M. Herz, of the Law Offices of Robert Herz, P.C. and hereby moves this court, pursuant to the fifth and sixth amendment of the United States Constitution, and as well Federal Rule of Criminal Procedure 16, and *Brady v.* Maryland, 373 U.S. 83 (1963) and its progeny, for an order compelling the government to provide discovery and produce evidence of a copy of the Torrential Downpour software used by the government in its undercover investigation in this case between October 20 and November 24, 2016, those dates being approximate.

BACKGROUND FACTS

A. The Indictment.

On April 26, 2019 the government filed a third superseding indictment in this case. Mr. Schwier was arraigned on the new indictment on May 1, 2019. Count 1 of the third superseding indictment reads as follows:

> On or about October 20, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did ***knowingly possess, and knowingly access*** with intent to view, any computer disk, and any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been mailed, and shipped and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that have been mailed, and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Any image of child pornography involved in the offense involved a prepubescent minor and a minor who had not attained 12 years of age. All of which is in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2).

Emphasis supplied.

Count 2 of the third superseding indictment reads as follows:

> On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, did **knowingly distribute** any child pornography, as defined in 18 U.S.C. § 2256(8)(a), that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. All of which is in violation of 18 U.S.C. § 2252A(a)(2)(A), (b)(1).

Emphasis supplied. Of note, in this iteration of the distribution count, the government simply claims that Mr. Schwier did "knowingly distribute *any* child pornography...." The government does not specify an image or provide a file designation nor describe the number of images distributed. However, the government will concede only one act of "distribution" allegedly transpired in this case when the FBI allegedly downloaded and

received one file alleged to contain child porn. A comparison of this iteration of the charge to how it was written in the Second Superseding Indictment is illustrative. Count 2 in the Second Superseding indictment reads as follows:

> On or about November 22, 2016, to November 24, 2016, within the District of Alaska, the defendant, MATTHEW WILLIAM SCHWIER, ***did knowingly distribute***, by any means and facility of interstate and foreign commerce, a visual depiction of a minor engaging in sexually explicit conduct, ***to wit: "1180842565051.jpg,"*** the production of which involved the use of minors engaging in sexually explicit conduct. The production of the visual depiction involved a prepubescent minor and minor under 12 years of age engaging in sexually explicit conduct and the visual depiction was of such conduct. All of which is in violation of 18 U.S.C. § 2252(a)(2), (b)(1).

Emphasis supplied.

As the court can see, in the Second Superseding Indictment the government specifies a single and sole image as allegedly distributed, and indeed, that is the only file the FBI claims that it ever downloaded and received, based on all the discovery provided by the government to date.

B. The Investigation

1. The October surreptitious searches.

According to SA Allison's affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about October 20, 2016 he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. This FBI modified program is only available to law enforcement and is known as "Torrential Downpour." This FBI program has never been scientifically validated or verified to be reliable by any

independent third party and shown to work in the manner claimed by the FBI. The FBI program attempted to download data, identified by a specific hash value, believed to contain child pornography. According to the agent, the hash value represents 3439 pieces of data representing a total of 66 files. Allegedly the target IP address "acknowledged" that it had 1387 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address "possessed" 45 of the files. According to the SA Allison 6 of these files contain child porn based on a review of archived FBI files. *None of those files were downloaded or received by the FBI.*

Later that same day, the FBI program made a second attempt to download data from the same target IP address. The attempt to download data again used an indentified hash value believed to contain child porn. This hash value, according to the agent, contains 6595 pieces of data and represents 249 files. Of these, the FBI program allegedly identified the IP address as having 6474 pieces of the data and 204 complete files. Based on a review conducted by SA Allison of FBI archived files, allegedly 74 of these files contain child porn. However, as before during the first attempt, *none of the 6474 pieces of data were downloaded or received by the FBI, and none of the files were downloaded or received by the FBI.* See, paragraphs 22-23 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

2. The November surreptitious searches. The FBI again experienced problems downloading files just as it had during the October 2016 surreptitious searches.

According to SA Allison's affidavit in support of the search warrant application, 3:17-mj-00198 DMS, dated April 28, 2017, on or about November 20, 2016 between 7:23 p.m. and 7:27 a.m. the next day, he conducted a surreptitious search of an IP address, later identified as being associated with Mr. Schwier. The agent attempted to

download data from the identified IP address, using an FBI modified program of the bitTorrent protocol. The FBI program attempted to download data, identified by specific hash values, believed to contain child pornography. According to the agent, the hash values represent 1545 pieces of data representing a total of 306 files. Allegedly the target IP address "acknowledged" that it had all 1545 pieces of data *none of which were downloaded or received by the FBI*. In addition, the modified FBI program allegedly reported that the IP address "possessed" all 306 of the files. According to SA Allison 28 of these files contain child porn based on his review of archived FBI files. *None of those files were downloaded or received by the FBI.*

On that same day, the FBI program made a second attempt to download data from the same target IP address between 7:43 p.m. and 8:26 p.m.. The attempt to download data again used an indentified hash value believed to contain child porn. This hash value, according to the agent, contains 543 pieces of data and represented one (1) file. The FBI program allegedly identified the IP address as having all 543 pieces of the data and the one (1) complete file. Based on SA Allison's review of FBI archived files, allegedly the one file contained child porn. However, as before, during the first attempt, *none of the 543 pieces of data were downloaded or received by the FBI, and none of the single file was downloaded or received by the FBI.* See, paragraphs 24-25 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS.

On November 22, 2016 a third search of the identified IP address was initiated. This third attempt to download data began on November 22 at 8:48 p.m. and ended on November 24, 2016 at 9:02 p.m. The attempt to download data again used an identified hash value believed to contain child porn. This hash value, according to the agent, contains 4861 pieces of data and represents 5616 files. Of these, the FBI program allegedly identified the IP address as having 4619 pieces of the data and 5309 complete

files. This time two files were completely downloaded and received by the FBI. No other pieces of data and no other files alleged to be "possessed" were downloaded or received by the FBI. Based on SA Allison's review of the two files received, only one file was determined by the agent to contain child porn. The file designation for that file is 1180842565051.jpg. See, paragraphs 26 of Affidavit of SA Allison filed in support of Search Warrant Application 3:17-mj-00198 DMS. It is this one file that forms the basis of count 2 in the Third Superseding Indictment.

C. The Forensic Search Of Mr. Schwier's Hard Drives.

1. The subsequent FBI search found nothing related to any putative data or files from October 20, 2016 on any of Mr. Schwier's computers or hard drives.

The search warrant application was granted by the court on April 28, 2017 and a search of Mr. Schwier's residence commenced on May 1, 2017. A number of electronic media were seized, including several computers containing internal hard drives, and some external hard drives as well. Subsequent to these items being seized they were forensically analyzed by Agent Allison. Agent Allison reported the results of this forensic evaluation in two "FBI 302s" dated respectively July 7 and July 12, 2017. None of the data or files, and no fragments of any of these files, allegedly identified as being "acknowledged" or "possessed" on October 20, 2016 were found on any media seized from Mr. Schwier. Moreover, AUSA Walker indicated during a hearing before this court on March 25, 2019, that for purposes of count 1 in the Second Superseding Indictment (which alleges the same conduct as in Third Superseding Indictment) that the government could not specify or identify the particular "matter' or hard drive seized from Mr. Schwier on which any contraband alleged to be possessed on or about October 20 was alleged to be found for purposes of count 1 of the indictment.

2. The subsequent FBI search of hard drives and computers seized from Mr. Schwier's residence found nothing related to any putative data or files from November 20, 2016 through November 24, 2016 on any of Mr. Schwier's computers or hard drives, including the one file allegedly "distributed."

None of the data or files, and no fragments of any of these files, allegedly identified as being "acknowledged" or "possessed" on or about November 20 to November 24, 2016 were found on any media seized from Mr. Schwier. There was no trace of the file allegedly downloaded and comprising the file designation 1180842565051.jpg that is the basis for count 2. Defense requests to have access to and to inspect and examine the original file on the original media upon which it was saved by the government when it was downloaded and that comprises 1180842565051.jpg have been denied by the government. The defense requires access to the original file to attempt to determine its actual origins and to authenticate it.

D. The BitTorrent Network and Torrential Downpour.

The indictment in this cases alleges that Mr. Schwier downloaded and shared child pornography files using the BitTorrent file-sharing network. BitTorrent is an online peer-to-peer network that allows users to download files containing large amounts of data, such as movies, videos, and music. Instead of relying on a single server to provide an entire file directly to another computer, which can cause slow download speeds, BitTorrent users can download portions of the file from numerous other BitTorrent users simultaneously, resulting in faster download speeds.

To download and share files over the BitTorrent network, a user must install a BitTorrent software "client" on his computer and download a "torrent" from a torrent-search website. A torrent is a text-file containing instructions on how to find, download, and assemble the pieces of the image or video files the user wishes to view. The client software reads the instructions in the torrent, finds the pieces of the target file from

other BitTorrent users who have the same torrent, and downloads and assembles the pieces, producing a complete file. The client software also makes the file accessible to the other BitTorrent users in a shared folder on the user's computer.

Torrential Downpour is law enforcement's modified version of the BitTorrent protocol. Torrential Downpour acts as a BitTorrent user and searches the internet for internet protocol ("IP") addresses offering torrents containing known child pornography files. When such an IP address is found, the program connects to that address and attempts to download the child pornography. The program generates detailed logs of the activity and communications between the program and the IP address. Unlike traditional BitTorrent programs, the government claims that Torrential Downpour downloads files only from a single IP address – rather than downloading pieces of files from multiple addresses – and does not share those files with other BitTorrent users.

E. The Investigations into Defendant's BitTorrent Activity.

As previously noted in October 2016, Agent Allison used Torrential Downpour to identify an IP address which allegedly was making known child pornography files available on the BitTorrent network. Agent Allison allegedly used Torrential Downpour to connect with this IP address to attempt to download child pornography files on several occasions between October 20, 2016 and November 24, 2016. Presumably had he successfully downloaded any files he would have reviewed the Torrential Downpour activity logs to confirm that the program downloaded complete files solely from this IP address, and would have reviewed the files to confirm that they were child pornography.

Through further investigation, Agent Allison learned the subscriber information for the IP address. He obtained a search warrant for the subscriber's residence, and FBI agents searched the residence on May 1, 2017. They found several items of computer

equipment including several hard drives; all of the equipment was then seized. Mr. Schwier has never made any admission that he had used any computer to knowingly find, download, view or distribute any child pornography. As noted before forensic examinations of the seized media failed to find any of the files allegedly possessed on October 20, or on November 20, or on November 22-24. The forensic examination performed by the FBI did reveal child pornography images on four of the hard drives seized; many of the images though were duplicative of each other. Almost all of the images were thumbnails in a thumbnail cache which could not viewed, manipulated, or distributed by anyone unless using a forensic toolkit available to law enforcement. Notably the file that Torrential Downpour allegedly had downloaded from the IP address was not found on any hard drive or any other seized device.

The government has charged Mr. Schwier with one count of distributing child pornography and three counts of possessing such material. The distribution count is based on the file that Torrential Downpour allegedly downloaded on or about November 22, 2016. The possession counts are based on the child pornography found on the hard drives after the search.

ARGUMENT

Mr. Schwier contends that the Torrential Downpour software is flawed and should be tested and verified by a third party. He also contends that he needs access to the program in order to prepare effective cross examination of Agent Allison and the potential presentation by his own computer expert. Mr. Schwier seeks disclosure of an installable copy of the software pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). He also seeks disclosure of Torrential Downpour's user and training manuals. He does not seek the program's source code.

Under Rule 16(a)(1)(E), the government must disclose any "books, papers, documents, data, . . . or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense[.]" To obtain disclosure under subsection (i), "[a] defendant must make a 'threshold showing of materiality[.]'" *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added); *see also Budziak*, 697 F.3d at 1111-12.

A. Brady v. Maryland

Brady v. Maryland, 373 U.S. 83 (1963), requires the government to disclose to a defendant any and all evidence favorable to him if the evidence is material to guilt or to punishment. The good or bad faith of the prosecution in withholding the evidence is irrelevant: it must be disclosed, even if doubtful, and failure to recognize the evidence does not save the prosecutor from a violation. *Id.* At 87; *Strickler v. Greene*, 527 U.S. 263 (1999); *Youngblood v. West Virginia*, 547 U.S 867 (2007). Under *Brady* and its progeny the "prosecution," which includes the prosecuting attorney as well as the investigating agencies, must disclose favorable information that is, or is known to be, in its possession. *Strickler* at 263; *Kyles v. Whitley*, 514 U.S. 419 (1995); *Jackson v. Brown*, 513 F.3d 1057 (9th Cir. 2008).

The duty of disclosure extends to evidence relating to the credibility of witnesses. *Strickler* at 263, *Giglio v. United States*, 405 U.S. 150, 154 (1972). The existence or nonexistence of a defense request for the evidence is immaterial to the

prosecution's duty to produce it. *Strickler* at 263; *United States v. Agurs*, 427 U.S. 97, 107 (1976). Even evidence the prosecutor regards as inherently improbable must be disclosed. *In re Chol Soo Lee*, 103 Cal.App.3d 615, 618-619 (1980). "Impeachment evidence … as well as exculpatory evidence, falls within the Brady rule." *United States v. Bagley*, 473 U.S. 667, 676 (1985). "When the 'reliability of a given witness may well be determinative of guilt or innocence' nondisclosure of evidence affecting credibility falls within this general rule." *Giglio v. United States*, 405 U.S. 150, 15355 (1972). Thus, the prosecution violates due process by "fail[ing] to disclose evidence that the defense might" use "to impeach the Government's witnesses by showing bias or interest." *Bagley*, 473 U.S. at 676. The information need not be admissible so long as it "is likely to lead to favorable evidence that would be admissible." *United States v. Sudikoff,* 36 F.Supp.2d 1196, 1200 (C.D. Cal 1999).

"The prosecution's duty to reveal favorable, material information extends to information that is not in the possession of the individual prosecutor trying the case." *Amado v. Gonzalez*, 758 F.3d 1119, 1134 (9th Cir. 2014). In particular, it extends to police officer witnesses. *See e.g., United States v. Price*, 566 F.3d 900, 903 (9th Cir. 2009) (reversing and remanding where federal prosecutors failed to learn of exculpatory evidence in the state police's control). The prosecution's duty also extends to situations where there is a dispute between the parties about the significance of the information. The prosecution should not "confuse[] the weight" to be given *Brady* evidence "with its favorable tendency." *Kyles*, 514 U.S. at 451. In order to qualify, the evidence need only have "some weight" that is "favorable" to the defense. *Id.* "[T]he Suprement Court has pronounced that if a prosecutor has doubt about certain evidence' exculpatory value, the prosecutor should err on the side of disclosure." *Schledwitz v. United States*, 169 F.3d 1003, 1014 n.4 (6th Cir. 1999)(citing Kyles); *United States v. Agurs*, 427 U.S. 97, 108

(1976); *see also United States v. Van Brandy*, 726 F.2d 548, 552 (9th Cir. 1984) ("[t]he government, where doubt exists as to the usefulness of evidence, should resolve such doubts in favor of full disclosure").

B. United State's Attorney Manual

In addition, the United States Attorney's Manual rigorously encourages prosecutors "to seek all exculpatory and impeachment information from all members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. U.S. Dept. of Justice, Justice Manual, § 9-5.001, "Policy Regarding Disclosure of Exculpatory and Impeachment Information." This policy guides federal prosecutors to probe carefully and to "disclose information that is inconsistent with any element of any crime charged against the defendant or that establishes a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal of the defendant for a charged crime." *Id.* at 9.5001.C. The manual provides for broad interpretation of "impeachment information": "A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make a difference between conviction and acquittal of the defendant for a charged crime" *Id.*

C. Discoverability of Investigative Software.

The Ninth Circuit has addressed the discoverability of government software programs used to investigate child pornography offenses.

Mr. Schwier relies primarily on *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), and cases that have adopted its reasoning. *Budziak* involved the FBI's use of an enhanced version of the LimeWire file-sharing program called "EP2P." *Id.* at 1107. Using that program, the FBI downloaded several child pornography files from an IP address registered to Budziak. *Id.* A forensic examination of his computer revealed multiple child pornography files, including several images the EP2P program had downloaded. *Id.* Budziak was charged with multiple counts of distributing and possessing child pornography. *Id.* The district court denied Budziak's motions to compel disclosure of the government's EP2P program, and he was convicted on each count. *Id.* at 1107-08.

On appeal, the Ninth Circuit held that the district court abused its discretion in denying Budziak's motions to compel. It noted that he did more than assert a generalized need to review the EP2P program before trial; he identified particular defenses to the distribution charges that discovery on the EP2P program could help him develop. *Id.* at 1112. Specifically, he "presented evidence suggesting that the 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 [the FBI]." *Id.* at 1112. He also presented "evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.* Given this evidence, the Ninth Circuit concluded that "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id.*

Other cases have followed *Budziak*. For example, the district court in *United States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at *7 (D.N.M. Apr. 3,

2013), required the government to allow the defense expert to examine and use a copy of the government's confidential Shareaza software at a secure government facility. The court did so because the defendant in *Crowe*, like the defendant in *Budziak*, presented specific evidence to suggest that access to the software was material to preparing the defense. *See id.* Specifically, the defense expert testified that "some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis." *Id.* See also, *U.S. v. Gonzales*, 2:17-cr-01311-DGC (D.AZ)(Order of court at Doc. 51, filed Feb.19, 2019, ordering disclosure of Torrential Downpour software); *U.S. v. Hartman*, 8:15-cr-00063-JLS (Cen.D. Cal)(Order of court at Doc. 87, filed Nov.24, 2015, ordering disclosure of government proprietary software Peer Spectre and ShareazaLE).

In *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015), the court of appeals affirmed a district court decision denying discovery of the "law enforcement tools" used to locate and download child pornography from the defendant's computer. The Sixth Circuit distinguished *Budziak,* noting that Budziak had presented the evidence just described *supra*. 787 F.3d at 365-67. The defendant in *Pirosko*, by contrast, "failed to produce any such evidence, simply alleging that he might have found such evidence had he been given access to the government's programs." *Id.* at 365. As a result, discovery was not warranted. *Id.*[1]

---

[1] *See also United States v. Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (affirming denial of motion to compel government software because the defendant was convicted of receiving and possessing child pornography and "the likelihood of any help to [his] defense was 'vanishingly small'"); *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012) (expressing no view on whether the EP2P source code was discoverable under Rule 16 where the defendant "neither contradicted nor cast the slightest doubt upon" the government's evidence that the FBI had downloaded child pornography from his computer); *United States v. Blouin*, 2017 WL 2573993, at *3 (W.D. Wash. June 14, 2017) (denying motion to compel

Budziak is, of course, binding precedent for this Court. The distinction between it and the *Pirosko* line of cases, just noted, is consistent with traditional Rule 16 principles. As already noted, "[n]either a general description of the information sought nor conclusory allegations of materiality suffice [under Rule 16(a)(1)(E)(i)]; a defendant must present *facts* which would tend to show that the [g]overnment is in possession of information helpful to the defense." *Mandel*, 914 F.2d at 1219 (emphasis added). In *Budziak* and *Crowe*, the defendants presented evidence to support their contention that discovery of the government software was material to preparing their defense to distribution of child pornography. In the other line of cases, they did not.

D. Mr. Schwier Has Shown Materiality.

Counts one and three allege violations of 18 U.S.C. § 2252A(a)(5)(B) and count two alleges a violation of 18 U.S.C. § 2252A(a)(2)(A). The latter section provides criminal punishment for any person who "knowingly receives or distributes, any child pornography ….. using any means or facility of interstate or foreign commerce . . . including by computer, . . ." Evidence is sufficient to support a conviction for distribution under § 2252A(a)(2) "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." *Budziak*, 697 F.3d at 1109.

---

where the defendant did not dispute that the government's software downloads files from a single source); *United States v. Maurek*, No. CR-15-129-D, 2015 WL 12915605 at *3 (W.D. Okla. Aug. 31, 2015) (denying motion to compel where the defendant failed to present specific facts which would tend to show how disclosure of Torrential Downpour would be material to his defense);

Mr. Schwier disputes and certainly casts doubt on whether the government downloaded any child pornography from any device possessed by him, and he disputes that Torrential Downpour consistently works as intended and is free from "bugs" so that it always and reliably downloads from a single source. Mr. Schwier maintains that Torrential Downpour is material to his defense because the distribution charge, Count 2, is based on a child pornography file that Torrential Downpour purportedly downloaded from his computer hard drive but that was not found on any hard drive or other device associated with Mr. Schwier when it was seized by the FBI. Torrential Downpour is also material to his defense because Count 1 specifically alleges he knowingly possessed child pornography on October 20 based on the surreptitious search conducted using Torrential Downpour. The government claims that the Torrential Downpour software allegedly identified and confirmed that child porn files were on a device using a specific IP address later found to be associated with Mr. Schwier. Yet none of those files or even fragments of those files were ever found on any device seized from Mr. Schwier's residence.

Mr. Schwier has presented an affidavit from his expert, Jeffrey M. Fischbach, confirming that the files are not on any device. Fischbach explains in his Declaration that it is critical to Mr. Schwier's defense to understand how Torrential Downpour functions in order to determine the program's reliability and accuracy in identifying the file that Mr. Schwier is charged with knowingly distributing or possessing. *Id.* at ¶ 29. He further states that based on his many years of research and testing of peer-to-peer file sharing software, including BitTorrent, he has discovered that all of these programs "contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable." *Id.* ¶ 22. Fischbach has opined that all software programs have flaws, and Torrential Downpour is no exception. He bases this opinion on his work in other cases involving Torrential

Downpour and the fact that the files the program allegedly downloaded in this case were not found on Schwier's devices. *Id.* at ¶ 21. Fischbach also provided a plausible explanation for how Torrential Downpour may have erroneously identified Schwier's computer as offering child pornography files over the BitTorrent network. Fischbach explained that, because a torrent is simply a text-file containing the hash values – or "fingerprints" – of the target image and video files, a BitTorrent user who downloads a torrent has fingerprints of the target files, even if he has not yet downloaded them. *Id.* at ¶ 15. Fischbach stated that the actual downloading of the target files occurs only when the client software instructs the torrent to search for those files on the BitTorrent network and download them to a designated folder on the user's computer. *Id.* at ¶ 14. He further stated that a forensic examination of the device used to download the torrent can determine whether the torrent has been used to download the file, and his examination of Schwier's devices revealed no evidence suggesting that he downloaded any files listed that might pertain to counts one through three. Id at ¶ 18. Fischbach opined that Torrential Downpour may have obtained the files from other BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing programs are designed to work. *Id.* at ¶ 17.

This evidence brings this case squarely within the holding of *Budziak*. Mr. Schwier has done more than simply request access to the software and argue that it is material to his defense. He has presented evidence that calls into question the government's version of events. Given his evidence, this Court must find that "the functions of the [program] constitute[] a 'very important issue' for [Schwier's] defense." *Budziak*, 697 F.3d at 1112 (quoting *United States v. Cedano-Arellano*, 332 F.3d 568, 571 (9th Cir. 2003)); *see Crowe*, 2013 WL 12335320, at *7.

Where a defendant has demonstrated materiality, the Court "should not merely defer to government assertions that discovery would be fruitless." *Budziak*, 697 F.3d at

1112-13. Mr. Schwier "should not have to rely solely on the government's word that further discovery is unnecessary." *Id.* at 1113. Because Mr. Schwier 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 Allison.[2]

Mr. Schwier also contends that Torrential Downpour is material because the program "searches beyond the public domain, essentially hacking computers as it searches for suspect hash values, and over-rides the computer's settings that otherwise would make files unavailable to be shared.

Mr. Schwier is charged with distributing child pornography based on the government's claim that the FBI, after apparently at some point identifying his computer as a download candidate for child pornography, infiltrated his computer on October 20, 2016 and attempted to download files. According to the Torrential Downpour software there were allegedly numerous suspect files on the computer. Yet, none of these attempts were successful. The FBI infiltrated his computer again in late November, again according to the software there were numberous suspect files on the computer. Again the FBI attempted to download files, and again all these attempts were unsuccessful, except for two suspect files that were successfully downloaded, and only one that was "verified" to be a prohibited image. Later when the computer hard drive was forensically searched, none of the identified suspected files that

---

[2] Even if the government were to present a log file purportedly showing that Agent Allison used Torrential Downpour to download from Schwier's device the child pornography file listed in count 2 of the Second Superseding Indictment, and that presumably forms the basis for count 2 in the Third Superseding Indictment, this log file cannot independently confirm that Agent Allison downloaded a complete child pornography file solely from Schwier's device. Since the log files were created by Torrential Downpour, if the program is flawed in the ways Schwier suggests, these log files would be flawed as well.

Torrential Downpour identified as being on the computer were found on the hard drive. Moreover, the one image that was "successfully" downloaded and "verified" to be a prohibited image also was not found on any hard drive possessed by Mr. Schwier.

The FBI could not find any of the files described by Torrential Downpour as being present and as described in the search warrant affidavit on any of the devices seized from Mr. Schwier. Apart from the allegation of "distribution" in the warrant affidavit, there is no evidence that Mr. Schwier ever physically distributed child pornography to another person. Mr. Schwier may defend the distribution allegation on the basis that he did not knowingly allow others to access files on his computer, and that Torrential Downpour overrode his computer's settings which were set so as to not share files on the BitTorrent software client. This defense requires access to the Torrential Downpour program. In identical circumstances, the Ninth Circuit ruled that defendant is entitled to discovery of special law enforcement software used to investigate him. *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). The court found disclosure of the government software was material to the defense to show that law enforcement may have downloaded only fragments of files from his "incomplete folder; to show that "agents could have used the EP2P software to override his sharing settings"; and because "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id* at 1112. The Court held that "the functions of the EP2P software constituted a 'very important issue' for Budziak's defense. Given that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense." *Id.*

Here, the sole evidence of distribution arises from Agent Allison's use of the Torrential Downpour program. This program has been described in testimony by one of its creators as follows:

> Torrential Downpour is a law enforcement surveillance software that is used exclusively by law enforcement. It is used to track, investigate, and eventually arrest those sharing child pornography through various P2P sharing networks…. Torrential Downpour is "somewhat unique" in that (1) it is designed to target and download files from a single IP address, as opposed to multiple sources, and restrict downloads to come from only that particular address (this is called a "single source download"): (2) Torrential Downpour creates a detailed log of events for evidentiary purposes; and (3) Torrential Downpour does not share files.

United States v. Maurek, 131 F. Supp. 3d 1258, 1261 (W.D. Ok. 2015). The indictment puts the use of this software squarely at issue by claiming that Mr. Schwier distributed child pornography when law enforcement downloaded child pornography from his computer or that he possessed child pornography when the software claimed it was he had it when in fact he did not. The government claims that Mr. Schwier's computer was the sole candidate for each download but acknowledges that BitTorrent software typically assembles a file from multiple sources.

In addition Mr. Schwier seeks disclosure of the "pooled information" that enabled the government to focus on the IP address later determined to be associated with Mr. Schwier.

Mr. Schwier also seeks copies of any license, training materials, user manuals, and instructions associated with the program, needed to effectively cross-examine the investigative officer and/or the government's expert as to their ability to use the program correctly and to testify about it. These materials may also aid in showing that the program was used in a manner that violated Mr. Schwier's rights.

The timing of the police investigation spanning October 2016 to April 2017 also strongly suggests there may have been times that police tried to download files and were unable to do so because sharing was precluded, either by features in the law enforcement software or for other reasons. Such evidence would tend to show that Mr. Schwier did not allow others to download from his computer. Such evidence is discoverable under *Brady* and should be disclosed.

Mr. Schwier also requests chain-of-custody documentation for any files the FBI claim to have downloaded, including but not limited all *meta*-data for any alleged downloaded file. Such documentation is a routine part of the impoundment process for digital evidence and should be provided.

CONCLUSION

Given the problems the FBI had successfully downloading and receiving any files, it is material to the defense of these charges to determine the actual origins of the file with the file designation 1180842565051.jpg. This file was not found on any digital media seized from Mr. Schwier's residence. At this time no known creation or access dates are known to exist for this file, and serious questions exist as to whether this file was ever on any media or device associated with Mr. Schwier. Given the manner in which BitTorrent normally works it is entirely possible this file did not come any device possessed by Mr. Schwier but rather was downloaded from another source. It is imperative that Mr. Schwier have access to the Torrential Downpour software to investigate this and to have access to the actual file as well for inspection and examination. Mr. Schwier has a constitutionally protected right to investigate the Government's claim that this file was downloaded from his computer. Production of the software and the file is essential to the defendant, and to properly preparing a defense and for proper cross-examination of the government's witnesses. Without such access

Mr. Schwier is denied the right to confront the evidence of which he is accused of possessing and distributing.

Respectfully, Mr. Schwier requests an order from the court compelling discovery and the production of the Torrential Downpour software.

DATED at Anchorage, Alaska, this 12th day of September 2019.

THE LAW OFFICES OF ROBERT HERZ, PC
s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171 / Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on September 12, 2019, a copy of the foregoing C- Motion to Compel Discovery and Production of Evidence was served electronically on Assistant United States Attorney's Office s/ Robert Herz