WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Anthony Espinoza Gonzales, Defendant.	No. CR17-01311-001-PHX-DGC **ORDER**

Defendant Anthony Espinoza Gonzales is charged with distributing and possessing child pornography in violation of 18 U.S.C. § 2252(a). Doc. 1. Following an evidentiary hearing on January 31, 2019, the Court granted in part Defendant's motion to compel disclosure of the Torrential Downpour software the FBI used in the investigation that led to his indictment. Doc. 51. Defendant moves to compel compliance with that order. Doc. 54. The motion is fully briefed (Docs. 55-56, 63-65, 81), and the Court held an evidentiary hearing on August 16, 2019 (Doc. 82). For reasons stated below, the motion is granted in part and denied in part.

I. Background.

The indictment alleges that Defendant distributed child pornography files on eight occasions in December 2016 and January 2017. Doc. 1 at 1-5. The government claims that Defendant downloaded and publicly shared the files using BitTorrent, an online peer-to-peer network that allows users to download files containing large amounts of data,

such as movies, videos, and music. 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 image or video files the user wishes to view. Once the torrent is downloaded to the BitTorrent client software, the software reads the instructions in the torrent, finds the pieces of the target files on the internet from other BitTorrent users who have the same torrent, and downloads and assembles the pieces, producing complete files. The client software also makes the pieces of the files accessible over the internet to other BitTorrent users by placing them in a shared folder on the user's computer.

The Torrential Downpour software is law enforcement's modified version of the BitTorrent protocol. The software is used to identify, on the BitTorrent network, internet protocol ("IP") addresses that have torrents associated with known child pornography files. When such an IP address is found, the software can be used to connect to that address and attempt to download child pornography.

II. The Court's Prior Order.

Defendant's computer forensics expert, Tami Loehrs, testified at the initial hearing in support of Defendant's motion to compel. Docs. 41, 50. FBI Agent Jimmie Daniels testified for the government. *Id.* Based in part on Loehrs's testimony, the Court found that Torrential Downpour is material to the defense under Rule 16(a)(1)(E)(i) because the distribution charges are based on child pornography files that Torrential Downpour purportedly downloaded over the internet from Defendant's computer, but that were not found on Defendant's computer when the FBI seized it pursuant to a search warrant. Doc. 51 at 8-10. The Court denied Defendant's request for a copy of Torrential Downpour under *Roviaro v. United States*, 353 U.S. 53 (1957), given Agent Daniels's testimony that the government's investigative efforts would be severely hampered if a copy got into the wrong hands. *Id.* at 14-15. But given the substantial defense interest established by Defendant, the Court concluded that Loehrs should be granted access to Torrential

Downpour to assist Defendant in preparing the defense. *Id.* at 15. The Court adopted the Rule 16 disclosure method authorized in *United States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at *8 (D.N.M. Apr. 3, 2013):

> [T]he defense expert [will be permitted] to examine the software at issue at a designated law enforcement facility, at a mutually convenient date and time, for as much time as is reasonably necessary for the expert to complete her examination. No copies of the software shall be made. The software shall not leave the custody of the law enforcement agency that controls it. Any proprietary information regarding the software that is disclosed to the defense expert shall not be reproduced, repeated or disseminated in any manner. Violation of [this] order shall subject the defense expert and/or defense counsel to potential sanctions by this Court.

Doc. 51 at 15.

Although the Court concluded that Loehrs should be permitted to examine Torrential Downpour given that the charged files were not found on Defendant's computer when it was seized, the Court rejected Defendant's argument that the software is material to a Fourth Amendment challenge because Defendant identified no evidence suggesting that the program accessed non-shared space on his computer. *Id.* at 10.

III. Defendant's Motion to Compel.

The parties corresponded regarding their proposed testing protocols for Torrential Downpour. Docs. 54-2, 54-3, 55-5. Based on the government's April 9, 2019 letter and the motion briefing, some issues have been resolved. A main point of contention is whether Loehrs may access during testing the Internet Crimes Against Children Task Force's Child Online Protection System ("COPS").

To determine the accuracy and reliability of Torrential Downpour, Loehrs proposes to perform nine tests: (1) non-parsed torrents, (2) partially-parsed torrents, (3) deleted torrent data, (4) unshared torrent data, (5) non-investigative torrents, (6) files of interest, (7) single source download, (8) detailed logging, and (9) restricted sharing. Doc. 56-1 at 21-24. Tests one through six would each conclude with a search of COPS for any investigative hits on the suspect IP address and determine whether Torrential Downpour

attempts to connect with that address to download data. *Id.* at 21-23. The government agrees to tests seven, eight, and nine, which do not involve COPS. Docs. 54-5 at 4, 55 at 2.

Tests one and two – non-parsed torrents and partially-parsed torrents – are relevant to whether Defendant downloaded complete files containing actual child pornography. The government does not address the potential materiality of these tests in its response to Defendant's motion. *See* Doc. 55.

The government objects to tests three and four because they would assess whether Torrential Downpour accesses non-shared space on the suspect computer, an issue the Court dealt with in its prior order when it rejected Defendant's argument that the software is material to a Fourth Amendment challenge. *Id.* at 3; *see* Doc. 51 at 10.

Loehrs wants to conduct tests five and six – non-investigative torrents and files of interest – to determine whether Torrential Downpour identified Defendant based solely on torrent files of investigative interest. Doc. 56-1 at 4, ¶¶ 11-12. But Defendant does not explain in his motion how this is material to the preparation of a defense.

To facilitate tests five and six, Loehrs requests that the COPS database be cloned and moved to a unique testing location on the server. Doc. 56-1 at 21. The new database would then be loaded with predefined lawful torrents known to be on the suspect computer, and Torrential Downpour would be directed to pull information from this "test database" and identify lawful files. *Id.* Loehrs claims that a test database should be used to avoid further dissemination of child pornography. *Id.*

The government objects to tests one through six, asserting that COPS must be protected from disclosure. Doc. 55 at 3-4. The government explains that public exposure of COPS could compromise child exploitation investigations worldwide because disclosure of the torrents being investigated by law enforcement would enable child pornographers to evade law enforcement detection and destroy evidence to thwart further investigation. *Id.* The government further explains that cloning and moving the COPS database, or building a separate database from which to do testing, would require a massive expenditure of resources. *Id.* at 4.

After reviewing memoranda filed by the parties, the Court directed them to provide supplemental briefing, with supporting affidavit testimony as necessary, to refine the issues and assist the Court in deciding Defendant's motion. Doc. 59. The parties filed the briefing in late June 2019 (Docs. 63-65), and Defendant filed an additional brief shortly before the August 16 hearing (Doc. 81). Loehrs testified at the hearing in support of Defendant's motion. Detective Robert Erdely, who helped create Torrential Downpour and is the current administrator of COPS, testified for the government. Doc. 82. Defendant filed a post-hearing brief on August 19. Doc. 85.

IV. Discussion.

A. Torrential Downpour and Its Interaction with COPS.

In its prior order, the Court described Torrential Downpour as follows:

> 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.

Doc. 51 at 2-3.

The government now explains that Torrential Downpour is really a suite of software whose components include (1) "Torrential Downpour Receptor," which the government claims is not involved in this case, and (2) the "Torrential Downpour program," which was used by Agent Daniels in this case. Doc. 64 at 2-4; *see also* Doc. 29 at 8-9 & n.7. Both components interact with COPS, but in different ways.

Torrential Downpour Receptor roams the internet and queries publicly available BitTorrent indices searching for IP addresses that have made public requests for specified torrent files that are of interest to law enforcement officers investigating child exploitative

file sharing activities. Doc. 64 at 2. Once Torrential Downpour Receptor detects an IP address associated with a torrent file of interest, it reports information about the IP address and the computer's networking port to COPS. *Id.* at 3. This information serves as a lead for officers to investigate using the Torrential Downpour program. *Id.*

The Torrential Downpour program has no search function. *Id.* Instead, officers use the program to initiate an investigation in one of two ways: (1) the program can interact with COPS in an automated fashion to obtain an investigative lead consistent with parameters an officer has set in the program – such as geographic area or a specific torrent – and the investigative lead is then loaded into the Torrential Downpour program (this is how Agent Daniels used Torrential Downpour in this case); or (2) officers can manually input an investigative lead – an IP address, networking port, and torrent – into the program. *Id.* Each option initiates Torrential Downpour's effort to connect to the suspect IP address and request a download of the files associated with the torrent. *Id.*

The government describes COPS as a repository containing information from various investigations conducted on several file sharing networks, including BitTorrent. *Id.* at 2. COPS is comprised of several servers that contain either "records in" – data received from Torrential Downpour Receptor – or "records out" – data that can be loaded into the Torrential Downpour program through a web portal used by investigating officers. *Id.* at 5. The data in COPS includes IP addresses and the "info hash" (unique identifier) of torrents being investigated by law enforcement officers around the world. *Id.* COPS also contains data relating to the identities and IP addresses of investigating officers. *Id.* COPS is updated by the minute with new information received from Torrential Downpour Receptor. *Id.* at 3.

B. The Government's Use of Torrential Downpour in this Case.

Agent Daniels set parameters in his Torrential Downpour program (v.1.33) to automatically request leads from COPS for his investigation. *Id.* at 3-4. Based on these settings, Torrential Downpour automatically downloaded information about Defendant's IP address, networking port, and the alleged torrents publicly shared by Defendant's IP

address. *Id.* at 4. Torrential Downpour then connected with Defendant's IP address and, the government alleges, downloaded the child pornography files that Defendant's computer was offering publicly from its shared folder. The downloaded child pornography is the basis for the charges in counts one through eight of the indictment. *Id.*; *see* Doc. 1 at 1-5.[1]

The government does not dispute that Torrential Downpour Receptor was used to initially identify Defendant's IP address and networking port as points of interest, or that it reported this information to COPS for further investigation. But the government objects to any testing of Torrential Downpour Receptor because Agent Daniels did not use the software in his investigation and the search results received by Torrential Downpour Receptor were not used as probable cause for the search warrant. Instead, the actual downloads of child pornography from Defendant's IP address through the Torrential Downpour program formed the basis for the search warrant request. The government also asserts that the search of the internet by Torrential Downpour Receptor will not be used by the government at trial. Doc. 64 at 4, 7-9, 11, 18.

C. Loehrs's Proposed Testing Protocol (Tests One Through Six).

1. Tests One and Two.

Loehrs describes test one as follows:

> [T]his first test simulates a scenario in which the Suspect Computer contains torrents, including legal torrents and torrents of investigative interest. However, none of the torrents have been parsed or seeded, meaning no associated files have been downloaded, so the Suspect Computer is void of the content of those torrents.

Doc. 56-1 at 21.

Loehrs explains that this test will determine whether Torrential Downpour identified Defendant based solely on a torrent that was never parsed, meaning the associated files were never downloaded to Defendant's computer. *Id.* at 3, ¶ 7. Loehrs claims that the

[1] Count nine charges Defendant with possessing other child pornography files found on his computer when it was seized pursuant to a search warrant. Doc. 1 at 5-6.

presence of a torrent alone, which is merely a text file that does not contain contraband, should not be identified by Torrential Downpour. *Id.*; *see also* Doc. 50 at 22-25.

Test two is similar to test one, but involves partially-parsed torrents. This is Loehrs's phrase for torrents where only some of the associated files were downloaded to Defendant's computer. Doc. 56-1 at 3, 21.

In response to questions from the Court at the August 16 hearing, the government acknowledged that Torrential Downpour Receptor, like all BitTorrent client software, will search the internet for torrents of interest and identify an IP address as a potential download candidate based on a non-parsed or partially-parsed torrent that has been loaded into the user's client software. Court's LiveNote Hr'g Tr. at 2:19-4:4, 20:20-22:18, 25:5-26:17 (hereinafter "Tr."). Torrential Downpour Receptor will then report the IP address to COPS for further investigation by law enforcement officers. *Id.* at 3:18-20. Loehrs confirmed that the purpose of tests one and two is to determine whether Torrential Downpour identifies a suspect IP address based solely on the address having a non-parsed or partially-parsed torrent. *Id.* at 6:13-16, 25:18-26:13; *see* Doc. 56-1 at 3, ¶¶ 7-8. Given the government's concession that this is how the software operates, tests one and two are not necessary. *See id.*

Defendant agreed at the hearing that test one is no longer necessary (Tr. at 6:8-16, 25:15-23), but argued that test two is still needed to determine whether Torrential Downpour Receptor identifies IP addresses based on a partially-parsed torrent containing no child pornography files or inadvertently downloaded files (*id.* at 7:5-8, 11:1-12:2). Defendant argued that he should not have to take the government's word as to how Torrential Downpour works. *Id.* at 13:1-7.

But to obtain discovery under Rule 16(a)(1)(E), Defendant "must make a 'threshold showing of materiality[.]'" *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012) (quoting *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). "Evidence is 'material' under Rule 16 if it is helpful to the development of a possible defense." *Id.* "'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 Government is in possession of information helpful to the defense.'" *Id.* at 1112 (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

Defendant expressed concern that Torrential Downpour Receptor may be identifying suspects based on lawful torrent files, citing testimony of one of Detective Erdely's colleagues. Tr. at 8:4-8, 9:23-10:8; *see* Doc. 81-1 at 8, ¶ 23. Based on her experience in other cases, Loehrs believes that COPS contains lawful torrent files, including cartoons, erotica, adult pornography, and images of children that are not sexual in nature. Doc. 63-1 at 5, ¶ 14.

But Defendant failed to explain why it would be helpful to his defense to show that Torrential Downpour Receptor identified his IP address, and put the address into COPS, based on lawful torrent files or inadvertently downloaded files. Defendant agreed that scanning the internet for publicly visible suspicious conduct does not constitute a Fourth Amendment search. Tr. at 11:19-22; *see also United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (defendant's expectation of privacy in his computer did not "survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program"); *United States v. Maurek*, 131 F. Supp. 3d 1258, 1262 (W.D. Okla. 2015) (numerous federal courts "have uniformly held there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file-sharing networks") (citations omitted). The fact that Torrential Downpour Receptor may have identified Defendant's IP address and put that address into COPS for further investigation on the basis of non-parsed or partially-parsed torrents related to child pornography, or Defendant's inadvertent receipt of a child pornography torrent, or even Defendant's possession of torrents that contain lawful adult pornography, is immaterial to the defense because scanning the internet for publicly available information, even lawful information, is not a Fourth Amendment violation.

Further, the charges in this case are not based on anything Defendant made available on the internet that was detected by Torrential Downpour Receptor. The charges are based

on what allegedly happened when the Torrential Downpour program followed up on the lead in COPS, contacted Defendant's IP address, and requested copies of child pornography his computer was offering to share publicly through the BitTorrent program. The government alleges that Defendant's computer shared the child pornography charged in the indictment on eight different occasions.

As noted, the government acknowledges that Torrential Downpour Receptor identifies a suspect IP address based on the address having a partially-parsed torrent. This is the fact test two seeks to establish. *See* Doc. 56-1 at 3, ¶ 8. Because this fact has been conceded by the government, and Defendant has not shown that test two is material to the defense for some other reason, the Court concludes that test two is not necessary.

2. Tests Three and Four.

Tests three and four involve scenarios in which the suspect computer contains deleted torrent files and torrents where the associated files have been moved to non-shared space on the computer. Doc. 56-1 at 21-22. The government asserts that the Torrential Downpour program does not access such non-shared space. Loehrs wants to test that assertion. *Id.* at 4.

The government objects to these tests based on the Court's rejection of Defendant's Fourth Amendment argument. Doc. 55 at 3. In his initial motion to compel, Defendant argued that Torrential Downpour is material to a potential Fourth Amendment violation because the program "searches beyond the public domain, essentially hacks computers searching for suspect hash values, and therefore conducts a warrantless search[.]" Doc. 25 at 6. The Court rejected this argument because Defendant identified no evidence that Torrential Downpour accessed non-shared space on his computer. Doc. 51 at 10.

The defense now proposes a different reason tests three and four are material – a scenario where Defendant started downloading files associated with a charged torrent, viewed some of these files and realized one of them contained contraband, and immediately deleted those files and stopped the download process. Doc. 63-1 at 2, ¶ 5. Loehrs asserts that it is important to "know if Torrential Downpour identified [the charged] files before

or after [Defendant] may have deleted them." *Id.* Loehrs states that the essential issue tests three and four will resolve "is whether Torrential Downpour is identifying files *after* a user has taken an affirmative action to delete them." *Id.* at 2-3, ¶ 6 (emphasis in original).

Detective Erdely testified that the Torrential Downpour program downloads only those files being shared by the user's BitTorrent software, and it is unlikely that µTorrent – the software Defendant used – would share files from non-shared space. Tr. at 31:8-24. Loehrs countered that BitTorrent software has been found to have exploits allowing it to access non-shared space, and she believes Torrential Downpour is susceptible to the same exploits. *Id.* at 37:12-21. Loehrs also stated that Torrential Downpour's instructions could have been modified to allow the program to access non-shared space. *Id.* at 33:7-20.

The distribution charges are based in large part on log files and Agent Daniels's testimony that the Torrential Downpour program downloaded child pornography files from shared space on Defendant's computer. Doc. 63 at 2. Defendant argues that he should not have to accept the government's word that the files were in shared space when identified by Torrential Downpour, particularly given that the files were not found on the computer when the FBI seized it. *Id.* The Court agrees. *See Budziak*, 697 F.3d at 1113.

"[E]vidence is sufficient to support a conviction for distribution under 18 U.S.C. § 2252(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." *Id.* at 1109. Thus, whether the Torrential Downpour program downloaded the charged files from shared space or non-shared space on Defendant's computer is material to the distribution charges. Defendant has made a sufficient Rule 16 factual showing to conduct tests three and four because the charged files were not found on his computer when it was seized by the government. Defendant will be permitted to conduct tests three and four (as modified below) to determine whether the Torrential Downpour program can access deleted or unshared torrent data. *See id.* at 1113.

/ / /

/ / /

3. Tests Five and Six.

Test five is a scenario in which the suspect computer contains non-investigative torrents and associated data. Doc. 56-1 at 22. Test six involves the use of files of investigative interest. *Id.* at 22-23. Loehrs explains that these tests will determine whether Torrential Downpour Receptor identifies torrents that contain lawful files. *Id.* at 4, ¶¶ 11-12; Doc. 63-1 at 4, ¶ 10. But as explained above, whether Defendant's IP address was identified by Torrential Downpour Receptor based on lawful files is not material to the defense. Even if that happened, the charges in this case are based on what Defendant's computer did when it was later contacted by Torrential Downpour.

Defendant claims that Torrential Downpour downloaded more than 30 files from his computer, only three of which were described by Agent Daniels as child pornography. Doc. 54 at 5; Tr. at 53:17-21. But Defendant is not charged with distributing lawful files. Each file charged in counts one through eight is alleged to contain images or videos of child pornography. *See* Doc. 1 at 1-5. And the Court can see no way in which Torrential Downpour's download of lawful files from Defendant's computer constitutes a defense to these charges. Distributing three videos containing child pornography along with 27 videos of lawful content still constitutes distribution of three videos of child pornography.

Moreover, the government acknowledged that Torrential Downpour investigates torrents relating to various child exploitation activities, and, in the process of downloading torrents known to contain child pornography, will sometimes download lawful files. Tr. 55:10-57:25. This acknowledgment renders tests five and six unnecessary. *See id.* at 51:7-52:4.

Defendant argued that the issue is whether the files were in fact downloaded from his computer as the government claims, and, if so, whether they were found in shared space. Tr. at 51:20-52:13, 54:9-13. But these issues will be addressed by tests three and four (deleted and unshared files) and test seven (single source download). *See id.* at 54:9-55:9, 60:4-61:7; Doc. 56-1 at 21-23.

Defense counsel further argued that she should be permitted to test Torrential Downpour thoroughly for any and all flaws, and posed a series of "what-if" scenarios as to how Torrential Downpour may work improperly. Tr. at 63:19-66:14. But to conduct discovery under Rule 16, Defendant must make a threshold factual showing of materiality. *See Budziak*, 697 F.3d at 1111. Fishing expeditions are not allowed. *See United States v. Chon*, 210 F.3d 990, 994 (9th Cir. 2000) (affirming denial of discovery request where the government had met its obligations under Rule 16 and "the requested discovery was a 'far reaching fishing expedition'"); *United States v. Spagnuolo*, 549 F.2d 705, 712-13 (9th Cir. 1977) (affirming denial of motion to compel under Rule 16 where the defendant merely assumed FBI files would show that his investigation was tainted by unlawful wiretaps and noting that he had "embarked on the type of fishing expedition condemned by [the] court in *Ogden v. United States*, 303 F.2d 724 (9th Cir. 1962)"); *United States v. Wolfenbarger*, No. 16-CR-00519-LHK-1, 2019 WL 3037590, at *8 (N.D. Cal. July 11, 2019) (denying discovery request in child pornography case and explaining that "Rule 16 does not authorize 'a shotgun fishing expedition for evidence'") (citation omitted). Defendant has made no threshold showing of materiality with respect to tests five and six.

D. Is Access to COPS Necessary to Conduct Tests Three and Four?

In her proposed testing protocol, Loehrs describes COPS and her request for access to the system as follows:

> [COPS] is a web-based component of Torrential Downpour and its operation including retrieving information about torrents of investigative interest and reporting historical data back to law enforcement for further investigation. Access to the [COPS] database will simulate law enforcement's undercover BitTorrent investigation by facilitating the same search capabilities relied upon in [this case].
>
> A unique login will be created by the government allowing access to the live [COPS] system in order to track and locate all information being reported by Torrential Downpour from the Suspect Computer, described below.

Doc. 54-4 at 8.

According to the government, Loehrs mistakenly believes that the COPS database includes a search function. Doc. 64 at 4. The government notes that Loehrs describes COPS as a component of Torrential Downpour and its operation, including "*retrieving information* about torrents of investigative interest and reporting historical data back to law enforcement for further investigation." *Id.* (quoting Doc. 56-1 at 17; emphasis by the government). Loehrs also states in her supplemental affidavit that the "COPS database is how the investigation into [Defendant] began." Doc. 63-1 at 3, ¶ 8. What Loehrs seems to be referring to, at least in part, is Torrential Downpour Receptor. *See* Doc. 70-1 at 12 (Detective Erdely's affidavit stating that it appears some of the tests proposed by Loehrs would use Torrential Downpour Receptor).

The government argues that access to COPS is not necessary or material for the limited examination of Torrential Downpour the Court has authorized. Doc. 64 at 4. The government states that the testing Loehrs seeks to run can be conducted by manually inputting IP addresses, port numbers, and lawful torrents into the Torrential Downpour program. *Id.* The government notes that law enforcement officers performed these functions manually prior to the automation of COPS, and can still do so today. *Id.* at 9.

At the hearing, Detective Erdely testified that when communicating with the Torrential Downpour program, COPS provides three pieces of information – an IP address, port number, and torrent – and Torrential Downpour then operates independently from COPS to investigate the IP address. Tr. 73:6-25, 78:17-20. He clarified that COPS also provides a preference for the order in which files are to be downloaded by Torrential Downpour (files of interest are to be downloaded first). *Id.* at 74:1-77:8. He explained that standard BitTorrent client software has a similar feature that allows the user to manually select the files to be downloaded. *Id.* at 74:10-12.[2]

[2] Defendant asserted that Detective Erdely "changed his story" about how COPS interacts with Torrential Downpour and this is a basis for providing Loehr's access to COPS. *Id.* at 78:8-11. Specifically, Defendant questioned why Torrential Downpour downloads lawful files at all if the program can target files known to contain child pornography. *Id.* at 12-16. Detective Erdely explained that the universe of child pornography is not known to law enforcement, and that files associated with torrents of interest are downloaded to determine whether they contain child pornography. *Id.* at

Loehrs asserts that COPS must be accessed "in its native state" for testing purposes, but does not explain why manually inputting IP addresses, port numbers, and torrents into the Torrential Downpour program, rather than having COPS do so automatically, will not allow for adequate testing of Torrential Downpour – the program Defendant has sought to investigate from the beginning and that allegedly downloaded the child pornography from Defendant's shared folder. Doc. 63-1 at 3, ¶ 8.

The government also provides credible evidence that cloning and moving the relevant portions of COPS, or creating a simulated database, is not feasible. Doc. 64 at 5-8. To clone and move the database would require considerable reprogramming because the COPS source code is not organized in a compartmented form, thus making it difficult to retrieve the portion dedicated solely to the BitTorrent network. *Id.* at 5. The government notes that the COPS database design includes various features, such as tables, database instances, and specific programming for retrieving data, that would be complicated to replicate. *Id.* at 5-6. The government estimates that cloning and moving the BitTorrent portion of COPS, and removing law enforcement sensitive data, would require more than 300 hours of work and cost between $75,000 and $100,000. *Id.* at 6. The government explains that creating a simulated version of COPS – a database that has taken nearly eight years to develop – would also be complicated and could involve dozens of hours of reprogramming. *Id.* at 6-7. The government notes that populating a simulated database manually is unnecessary because a database is simply a repository of information, something that can be accomplished by populating a local log file on Loehrs's computer. *Id.* at 7-9.[3]

For several reasons, the Court will not grant Defendant access to the COPS database.

First, Defendant has not shown that access to COPS is necessary to perform tests three and four. The question in those test is how Torrential Downpour interacts with a

79:1-22. The Court found Detective Erdely credible in describing how COPS and Torrential Downpour interact.

[3] In his hearing memorandum, Defendant proposes giving Loehrs a limited log-on to COPS, similar to allowing someone limited access to online bank accounts. Doc. 81 at 5. The government made clear that COPS contains no such feature. Tr. 71:2-6.

suspect computer – whether it accesses deleted files or non-shared space. The Court is satisfied that the question can be answered by manually loading the IP address, port number, and torrent information into the Torrential Downpour program and then observing how the program interacts with the suspect computer. Access to COPS is not required to conduct this test.[4]

Second, Defendant has not shown that access to COPS is material to preparation of his defense as required by Rule 16. As discussed above, further investigation of how the government searches the internet for publicly-offered child pornography will not aid the defense because such public searches do not violate the Fourth Amendment and the government does not intend to present evidence regarding Torrential Downpour Receptor at trial. Similarly, further investigation of the COPS database where Torrential Downpour Receptor deposits its investigative leads is not material. The government has presented credible evidence that COPS is simply a data base, not a search engine that conducted investigative activities in this case, and Defendant provides no facts to suggest otherwise.

Third, the Court concludes that COPS is protected from disclosure by the *Roviaro* privilege. The government has a legitimate interest in preserving its ability to investigate and prosecute the distribution of child pornography. COPS contains highly sensitive information about thousands of ongoing investigations into child pornography worldwide. Doc. 64 at 12; Tr. at 71:7-11. The information includes info hash data for the torrents of interest, and the IP addresses of both suspects and investigating officers. *Id.* The Court concludes that the substantial government interest in protecting the secrecy of COPS outweighs Defendant's need to access the database.

Fourth, although Rule 16 permits defendants in criminal cases to obtain discovery of certain categories of information in the government's possession or control, Rule 16 does not require the government to create information for a defendant. *See United States*

[4] The defense suggested at the hearing that COPS may provide instructions to the Torrential Downpour program that prompt it to look at deleted files or non-shared space on the suspect computer, but this suggestion appears to be pure speculation. The defense provides no facts to support this suggestion, and facts, rather than speculation, are required to obtain discovery under Rule 16. *See Budziak*, 697 F.3d 1112.

v. Hamzeh, No. 16-CR-21, 2019 WL 1331639, at *4 (E.D. Wis. Mar. 25, 2019) ("[A]lthough Rule 16(a)(1)(E) requires the government to disclose evidence, it does not require the government to create evidence."); *United States v. Mahon*, No. CR-09-0712-PHX-DGC, 2011 WL 5006737 at *3 (D. Ariz. Oct. 20, 2011) (citing cases). The Court can find no basis for requiring the government to incur the substantial time and expense required to clone or recreate the COPS database for Defendant's investigation.

V. Conclusion.

Tests one and two are not necessary because the government acknowledges that Torrential Downpour Receptor identifies IP addresses based on non-parsed and partially-parsed torrents. Tests three and four are material to the defense, but Loehrs is not permitted access to COPS in performing the tests. Tests five and six are not permitted because they are immaterial and unnecessary. The government has agreed to tests seven, eight, and nine.

IT IS ORDERED:

1. Defendant's motion to compel compliance with the Court's February 19, 2019 order (Doc. 54) is **granted in part and denied in part** as set forth in this order.

2. Defendant's motion to submit his supplemental brief (Doc. 85) is **granted**.[5]

3. Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to run from 4/15/2019.

Dated this 27th day of August, 2019.

David G. Campbell
Senior United States District Judge

[5] Defendant asserts in his brief that the "handshake" communication between Torrential Downpour and a suspect's computer can turn into an ongoing investigation that lasts an extended period of time (Doc. 85 at 2-7), but does not explain why this renders "all nine tests" material to the defense (*id.* at 7).