IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. MATTHEW WILLIAM SCHWIER, Defendant.	Case No. 3:17-cr-00095-SLG

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

Before the Court at Docket 199 is Defendant Matthew William Schwier's C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour Software. The government responded in opposition at Docket 214 and filed supplemental briefing at Docket 219. Mr. Schwier filed supplemental briefing at Docket 221. An evidentiary hearing was held on October 17 and 18, 2019.

BACKGROUND AND PROCEDURAL HISTORY

On October 20, 2016, the Federal Bureau of Investigation ("FBI") used software called "Torrential Downpour" to purportedly identify Mr. Schwier's computer as possessing child pornography files that were available for download by third parties through BitTorrent, a peer-to-peer file-sharing network.[1] Torrential

[1] Docket 199 at 6; Docket 214 at 3. As described by Robert Erdely—offered by the government as an expert witness—a peer-to-peer network "allow[s] individuals unknown to each other and possibly separated by great distances to share files, such as audio and video files, freely." Docket 214-1 at 2, ¶ 7 (Decl. of Mr. Erdely).

Downpour is a piece of software developed for law enforcement personnel, to allow them to identify BitTorrent users who possess or seek to possess child pornography files.[2] The software operates similarly to other BitTorrent clients—like uTorrent, the program Mr. Schwier allegedly used[3]—with several important differences.[4] Unlike most BitTorrent clients, Torrential Downpour allows law enforcement to download files from a single user,[5] and does not itself share any files downloaded pursuant to an investigation.[6] On October 20, 2016, Torrential Downpour was unable to download the alleged child pornography available for distribution on Mr. Schwier's computer.[7]

In November 2016, the FBI again used Torrential Downpour to identify Mr. Schwier's computer as possessing child pornography that was available for download.[8] Over the course of three days, the FBI used Torrential Downpour to

[2] Docket 214-1 at 5, ¶ 16.

[3] Docket 214 at 3.

[4] Docket 214-1 at 5–6, ¶¶ 18–20.

[5] Docket 214-1 at 6, ¶ 19. "Traditionally, BitTorrent seeks to download from many sharing computers to speed up the download times." Docket 214-1 at 6, ¶ 19.

[6] Docket 214-1 at 6, ¶ 20.

[7] Docket 199 at 3–4; Docket 214 at 4.

[8] Docket 199 at 4–6; Docket 214 at 5.

download two files shared by Mr. Schwier's computer, one of which allegedly contained child pornography.[9]

In May 2017, the FBI seized multiple pieces of hardware from Mr. Schwier's home while executing a search warrant.[10] Forensic examination of the hardware identified multiple child pornography files, but could not find the particular files identified or downloaded by Torrential Downpour in October and November 2016.[11]

On August 16, 2017, the grand jury indicted Mr. Schwier on three counts of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).[12] A September 25, 2017 superseding indictment additionally charged Mr. Schwier with one count of distribution of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).[13] On April 24, 2019, the grand jury returned a Third Superseding Indictment that charged Mr. Schwier with two counts of possession of child pornography and one count of distribution of child pornography.[14]

---

[9] Docket 199 at 6; Docket 214 at 5.

[10] Docket 199 at 6; Docket 214 at 6.

[11] Docket 199 at 7; Docket 214 at 6.

[12] Docket 2.

[13] Docket 40 at 3 (Count 3).

[14] Docket 138. A Second Superseding Indictment had been filed on March 20, 2019. Docket 117.

The FBI's October 20, 2016 use of Torrential Downpour to identify child pornography files on Mr. Schwier's computer forms the basis of Count 1 in the Third Superseding Indictment.[15] The FBI's use of Torrential Downpour to download child pornography from Mr. Schwier's computer in November 2016 forms the basis of Count 2 in the Third Superseding Indictment.[16] Count 3 of the Third Superseding Indictment relates to the child pornography files found during the 2017 physical search of Mr. Schwier's hardware and is not related to the FBI's use of Torrential Downpour.[17]

Mr. Schwier retained Robert M. Herz, his current defense counsel, on March 12, 2018.[18] Mr. Herz retained Jeffrey M. Fischbach as an expert in computer forensics at least as early as November 2018.[19] Despite this, Mr. Herz did not file the instant motion to compel production of the Torrential Downpour software—the

[15] Docket 199 at 6; Docket 214 at 3–4.

[16] Docket 199 at 6; Docket 214 at 5.

[17] Docket 138 at 3.

[18] Docket 63.

[19] Docket 203-1 at 2, ¶ 4 (Decl. of Mr. Fischbach) (describing Mr. Fischbach's November 2018 request to review alleged child pornography file downloaded from Mr. Schwier's computer). And Mr. Schwier's supplemental briefing indicates that Mr. Fischbach had begun developing his thoughts about "[t]he circumstances to be tested" should he gain access to Torrential Downpour in May 2019. Docket 221 at 5.

foundation for two counts in the Third Superseding Indictment—until September 12, 2019, one month before trial was scheduled to begin.[20]

DISCUSSION

Mr. Schwier contends that Torrential Downpour "is flawed and should be tested and verified by a third party," and that the defense requires access to the program in order to effectively cross-examine government witnesses.[21] Mr. Schwier seeks disclosure of an installable copy of Torrential Downpour, along with its user and training manuals.[22] He does not seek disclosure of Torrential Downpour's source code.[23]

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E)(i), the government must disclose any "books, papers, documents, data . . . or copies or portions" thereof upon the defendant's request, provided that the item is in the government's control and is "material to preparing the defense."[24] "A defendant

---

[20] Docket 199; Docket 175 (setting trial date for October 15, 2019).

[21] Docket 199 at 9.

[22] Docket 199 at 9.

[23] Docket 199 at 9. However, Mr. Fischbach did request a copy of the Torrential Downpour source code during his testimony. Docket 229 at 3:2–18 (Excerpt of 10/17/2019 Evidentiary Hearing Tr.). The Court denies that request for the reasons discussed below.

[24] The defense also bases its motion on the Supreme Court's decision in *Brady v. Maryland*, 373 U.S. 83 (1963). The Court finds that case inapplicable and denies Mr. Schwier's motion to the extent it seeks disclosure of Torrential Downpour under *Brady*. *See United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *7 (D. Ariz. Feb. 19, 2019) (discussing applicability of *Brady* and finding that

must make a 'threshold showing of materiality' in order to compel discovery pursuant" to this rule.[25] "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."[26]

In *Budziak*, the Ninth Circuit held that a district court had erroneously denied discovery of EP2P, a piece of investigative software similar to Torrential Downpour.[27] The Circuit concluded that the defendant had demonstrated materiality by "identif[ying] specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop."[28] The defense has done the same here; he presented evidence, through the declaration and testimony of Mr. Fischbach, suggesting that Torrential Downpour may have "exploit[ed] vulnerabilities in the [BitTorrent] protocols" to download files that Mr.

"[d]efendants have made no showing that Torrential Downpour will prove to be exculpatory or could be used to impeach a government witness").

[25] *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)).

[26] *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)).

[27] *Id.* at 1111–12.

[28] *Id.* at 1112.

Schwier had not made available for sharing.[29] Discovery of Torrential Downpour, then, could potentially help Mr. Schwier develop a defense to the distribution charge, as it is based solely on the FBI's use of the program to download files from Mr. Schwier's computer in November 2016.[30] Mr. Fischbach further explained, "it is critical to the defense . . . to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as 'publicly available,'"[31] since Torrential Downpour's alleged October 20, 2016 identification of child pornography files on Mr. Schwier's computer is the sole basis for one of the possession charges.[32]

In light of this, the Court finds that Mr. Schwier has made the threshold showing of materiality required by Rule 16.[33] The Court further finds that the materiality of Torrential Downpour is limited to versions 1.15 and 1.23 of the

---

[29] Docket 200-1 at 7–8, ¶¶ 20–23; *see also Budziak*, 697 F.3d at 1112 ("[The defendant] submitted evidence suggesting that the FBI agents could have used EP2P software to override his sharing settings.").

[30] *See Budziak*, 697 F.3d at 1112 ("Given that the distribution charge . . . was premised on the FBI's use of the EP2P program to download files from [the defendant], it is logical to conclude that the functions of the program were relevant to his defense.").

[31] Docket 200-1 at 8, ¶ 24.

[32] Docket 200-1 at 9, ¶ 26; *see also Budziak*, 697 F.3d at 1112 (explaining that "[l]ike the competency of the drug-sniffing dog in [*United States v. Cedano-Areliano*, 332 F.3d 568, 571 (9th Cir. 2003)] the functions of the EP2P software constituted a 'very important issue' for Budziak's defense").

[33] *See Budziak*, 697 F.3d at 1112.

software—the versions used by the FBI during the events underlying the relevant counts in the Third Superseding Indictment.[34]

The government argues that even if the functionality, reliability, and accuracy of Torrential Downpour is material, disclosure of the software itself should be precluded by what it terms as a "law enforcement privilege."[35] In *Rovario v. United States*, the Supreme Court recognized the government's "privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law."[36] The Supreme Court explained that "no fixed rule with respect to disclosure is justifiable" and directed courts to balance the public interest against the defendant's right to prepare his case, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors."[37] Courts have since applied this law enforcement privilege to investigative software like Torrential Downpour.[38]

---

[34] Docket 229 at 2:6–11.

[35] Docket 214 at 8–11.

[36] 353 U.S. 53, 59 (1957).

[37] *Roviaro v. United States*, 353 U.S. 53, 62 (1957).

[38] *See, e.g.*, *United States v. Pirosko*, 787 F.3d 358, 365–67 (6th Cir. 2015) (discussing the ShareazaLE software); *United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019) (discussing Torrential Downpour).

In *United States v. Gonzales*, the U.S. District Court for the District of Arizona recently applied the *Rovario* balancing test to Torrential Downpour, concluding that disclosure of an installable copy of the software to the defense was not warranted:

> Child pornography is a scourge, victimizing the most innocent for the basest of reasons. The government has a legitimate interest in preserving its ability to investigate and prosecute distribution of this material—distribution that creates the market and fuels the demand for creation of more child pornography. Agent Daniels testified that the government's investigative efforts would be severely hampered if a copy of Torrential Downpour got into the wrong hands. Countermeasures could be developed that would thwart law enforcement's monitoring of the BitTorrent network for suspected child pornography.[39]

The district court in *Gonzalez* did, however, allow the defense's expert to conduct certain testing of Torrential Downpour in a controlled setting at a secure government facility.[40]

The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that "child pornography distributors could find a way to avoid detection" if the workings of Torrential Downpour were made public, "render[ing]

---

[39] No. CR-17-01311-001-PHX-DGC, 2019 WL 669813, at *8 (D. Ariz. Feb. 19, 2019).

[40] *Id.*; *see also United States v. Gonzalez*, No. CR-17-01311-001-PHX-DGC, 2019 WL 4040531, at *4–7, *10 (D. Ariz. Aug. 27, 2019) (specifying which tests the defense was permitted to run). The government's proposed validation protocol in this case tracks the August 2019 *Gonzalez* testing closely. *See* Docket 219 at 3 (comparing *Gonzalez* tests and government's proposed validation protocol); *see also* Docket 219-1 (government's proposed validation protocol).

that tool of law enforcement ineffective."[41] At the evidentiary hearing, Mr. Erdely testified that "to give [the defense] unfettered access to this software puts law enforcement and ten years of development at risk" because it would reveal certain aspects of Torrential Downpour's operation.[42]

Given the government's strong interest in retaining control of Torrential Downpour, the Court finds that disclosure of the software itself is not warranted, at least as of this juncture. The government has proposed to allow the defense to examine Torrential Downpour's operation while it is run by a government expert in a controlled environment.[43] Mr. Erdely testified that this validation process, which includes packet capture by a program called "Wireshark," would address the defense's questions about Torrential Downpour's functionality, accuracy, and ability to exploit vulnerabilities in the BitTorrent protocol.[44]

The Court acknowledges Mr. Schwier's interest in understanding the operation of Torrential Downpour as it relates to his defense, and the Court concludes based on the present record that the validation process proposed by

---

[41] Docket 214-1 at 7, ¶ 23.

[42] Docket 230 at 8:25–9:2 (Excerpt of 10/18/2019 Evidentiary Hearing Tr.). *But see* Docket 221 at 2–3 (defense argument that Mr. Fischbach is trustworthy and is "a firewall" that will prevent Torrential Downpour's dissemination to the public).

[43] *See* Docket 219-1 (proposed validation process).

[44] Docket 230 at 9–17; *see also* Docket 230 at 10:24–11:5 ("[I]f there was a vulnerability and our software was designed to exploit these vulnerabilities, . . . it would be exposed in the Wireshark packet capture.").

the government is sufficient to meet the defense's needs. Mr. Fischbach had multiple opportunities to identify specific deficiencies in the government's proposed validation protocol, but was not able to do so in a way that persuaded the Court that additional or more extensive testing was necessary.[45] Mr. Fischbach testified that the proposed testing would not show how two features of Torrential Downpour—single-source downloading and the inability to upload—affect the BitTorrent protocol, if at all.[46] But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege.[47] And while the defense contends that it has begun to formulate tests for Torrential Downpour that may be helpful to the defense, it has not identified these tests or explained how they differ from the government's

[45] Docket 230 at 2–8 (Mr. Fischbach discussing the government's proposal). Mr. Fischbach, in his first declaration, expressed a concern that Torrential Downpour was exploiting vulnerabilities in either BitTorrent itself or in BitTorrent clients, such as uTorrent. Docket 200-1 at 7, ¶¶ 20–21. But Mr. Erdely persuasively testified that the specific uTorrent exploit identified by Mr. Fischbach had been resolved in 2014, well before the events of this case. Docket 214-1 at 12, ¶ 33. Moreover, as explained above, Mr. Erdely also persuasively testified that the use of packet capture, as specified in the government's proposed validation protocol, would reveal whether Torrential Downpour exploited any vulnerabilities. Docket 230 at 10:24–11:5.

[46] Docket 230 at 3:20–4:2, 6:3–16.

[47] Docket 230 at 6:24–7:4 ("[T]he findings that we have, and, again, I'm being careful as far as privilege goes, the findings that we have have demonstrated some oddities possibly, but, again, they have to be tested to see if they are associated, but they certainly cause concern.").

proposed validation protocol, claiming that the defense's proposed testing ideas are confidential attorney work product and subject to the attorney-client privilege.[48]

The Court cannot rule on the materiality of forensic tests that have not been disclosed to it. But the Court will accord the defense one last opportunity to explain what additional testing it is seeking and why. Accordingly, within **seven days of this order**, the defense may file a supplemental declaration of its expert that: (1) explains the specific hypotheses the defense seeks to test; (2) describes with particularity the test(s) the defense seeks to conduct; and (3) identifies the specific hardware and configurations necessary to complete that testing. The declaration shall also clearly explain why the government's proposed validation testing would not be adequate. This declaration may be filed ex parte or redacted, but only to the extent necessary to protect confidential attorney work product and/or privileged attorney-client communications.

CONCLUSION

In light of the foregoing, the motion at Docket 199 is GRANTED IN PART and DENIED IN PART.

IT IS HEREBY ORDERED that the validation process described at Docket 219-1 shall be carried out for versions 1.15 and 1.23 of the Torrential Downpour

[48] Docket 221 at 5–6; *see also* Docket 221 at 4 ("The defense in this case wants to run a specific examination to test for a particular hypothesis, a particular condition that the defense believes it may have uncovered.").

software on November 4, 2019, and on November 5, 2019 as necessary. The validation shall take place in a secure setting at a government location in Anchorage, Alaska that is selected by the government. Defense counsel and Mr. Fischbach may be present and may observe the validation process.

As discussed on the record,[49] the Court further enters a protective order with regard to the validation process as follows:

1. Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.
2. Nothing herein shall prevent either the government or the defendant from referencing the technical specifications of the software or any other materials in connection with pleadings or motions filed in this

[49] Docket 230 at 8:14–20.

case, provided the materials are filed under seal and/or submitted to the Court for *in camera* inspection.

3. Violation of this protective order may be punishable by contempt of court, whatever other sanction the Court deems just, and/or any other sanctions which are legally available.

In the event a timely supplemental expert declaration is filed by the defense, the Court may amend this order as warranted after the government has had an opportunity to respond.

DATED this 24th day of October, 2019, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE