IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CRIMINAL NO. 2:16cr36**
	)	
GERALD ANDREW DARBY,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO COMPEL

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, Elizabeth M. Yusi, Assistant United States Attorney, and Leslie Williams Fisher, United States Department of Justice Trial Attorney, and submits its response in opposition to the defendant GERALD ANDREW DARBY's Motion to Compel Discovery. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

Defendant GERALD ANDREW DARBY ("the defendant") is charged in this case with receipt and possession of child pornography. The charges arise from an investigation into Playpen, a website through which registered users like the defendant regularly accessed illegal child pornography. That website operated on the Tor network. This network allows its users to mask their Internet Protocol ("IP") addresses, which—absent such concealment—ordinarily can be used to identifying website users. The Tor network operates to conceal this information by bouncing user communications around a network of computers before transmitting such communications to their ultimate destination. The defendant's IP address was discovered through the court-authorized use of Network Investigative Technique ("NIT"). Pursuant to a search warrant authorized in this District, Playpen's content—which was hosted on a computer

server located within the district—was augmented with additional computer instructions comprising the NIT while the website briefly operated under government control.[1]

The defendant seeks disclosure of what he generally describes as the "source code or programming code for the NIT" used to identify his computer. Def.'s Mot. to Compel Disc. at 1. His request to compel disclosure of this information is untimely and represents nothing more than a fishing expedition for information that either is not material to his defense or has already been provided. Defendant does not meet the Fourth Circuit standard for materiality and incorrectly relies on the Ninth Circuit standard in his materiality claim. Moreover, even if the Court were to find that disclosure of the NIT programming code was material to his defense, that information is protected by a qualified law enforcement privilege. Accordingly, this Court should deny the defendant's motion.

BACKGROUND

I. Procedural History

On March 10, 2016, a federal grand jury sitting in Norfolk returned an eight-count indictment charging the defendant with five counts of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), and three counts of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4). At his arraignment, the Court set a preliminary motions deadline of April 13, 2016, and a trial date of May 24, 2016. Since that time, the trial has been continued until October 18, 2016.

[1] Further detail about the website, investigation, and NIT is contained in the government's Response to the Defendant's First Motion to Suppress and exhibits thereto (ECF 16). Such information is incorporated here by reference.

II. Discovery Requests and the government's Responses

On March 23, 2016, the parties entered an agreed discovery order. ECF 14. The government provided discovery pursuant to that order. Among the items included in that disclosure were materials pertaining to the investigation such as investigative reports and forensic report regarding the defendant's digital devices. In addition, the defendant's computer media has been available for inspection by a defense expert. However, defendant has not requested to review the devices. Defendant has not requested any additional discovery, including the "source code" that he now requests in his Motion to Compel.

Had the defendant requested the information he now seeks, the government would have advised that the information sought did not consist of evidence the government intended to use in its case-in-chief at trial and that such information had not been obtained from and did not belong to the defendant. The government would further advise that it did not believe that information was material to his defense. The government would also have advised that the investigative technique is subject to law enforcement privilege, which the government asserts. Pursuant to a proposed discovery protective order, the information collected through the use of the court-authorized NIT is available for counsel's review and will remain available for further review during the pendency of the litigation. The government will also provide the defendant a copy of that information subject to the entry of a protective order.

Additionally, regarding the NIT results, only a limited set of information was collected through court-authorized use of the NIT; specifically, the information described in Attachment B of the warrant authorizing the deployment of the NIT. See Govt. Resp.to First Mot. to Supp., Ex. A. Other information about user activity, such as the pages and postings accessed, had been collected through request data and website logs that were not a function of the NIT. *Id*. In this

response, the government offered to make additional information available to the defendant, including an offline copy of Playpen that would enable the defense team to navigate through pages of the website as a user could when the website was online. *Id*.

On April 13, 2016, the defendant filed two motions to suppress and also requested a *Franks* hearing. The government filed responses to the motions to suppress on April 27, 2016. The Court held a hearing on defendant's motions and denied the motions to suppress on June 3, 2016. Without leave of the Court to file a motion beyond the motions deadline, on June 2, 2016, defendant filed the instant motion to compel discovery.

LAW AND ARGUMENT

The defendant's motion to compel disclosure of the NIT source code is untimely because he filed it after both of the pretrial motions deadlines had passed and he did not seek leave to file an untimely motion. Regardless, if the defendant had timely filed his motion, he has not shown why the information he seeks is material to either his pretrial motions or to his defense. Moreover, the information that the defendant seeks to compel is subject to a qualified law enforcement privilege.

I. The Defendant has Failed to Show that the NIT Programming Code is Material to his Defense

Under Federal Rule of Criminal Procedure 16, a criminal defendant has a right to inspect documents, data, or tangible items within the government's "possession, custody, or control," that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). "[I]n the context of Rule 16, 'the defendant's defense' means the defendant's response to the government's case in chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996). "[E]vidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal."

United States v. Caro, 597 F.3d 608, 621 (4th Cir. 2010) (quoting *United States v. Lloyd*, 992 F.2d 348, 351 (D.C. Cir. 1993)).

The defendant bears the burden of showing that information sought under Rule 16 "would . . . actually help[] prove his defense." *Id*. To show materiality under Rule 16 "[t]here must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant to significantly alter the quantum of proof in his favor." *Id*. (quoting *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975)). A defendant cannot meet this burden through "general description[s] of the information sought" nor through "conclusory allegations of materiality." *Id*. (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)). In fact, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion, and for it to ignore the requirement is to abuse its discretion." *Mandel*, 914 F.2d at 1219. "[O]rdering production by the government without any preliminary showing of materiality is inconsistent with Rule 16." *Id*. Moreover, Rule 16 does not authorize a defendant to embark on a fishing expedition, which is exactly what the defense requests amounts to. *See United States v. White*, 450 F.2d 264, 268 (5th Cir. 1971); *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012); *United States v. Delacruz*, No. Case 14 Cr. 815 (KBF), 2015 WL 2211943, at *1 (S.D.N.Y. May 12, 2015) ("Rule 16 does 'not entitle a criminal defendant to a 'broad and blind fishing expedition among [items] possessed by the government on the chance that something impeaching might turn up.'" (quoting *United States v. Larranga Lopez*, No. 05 Cr. 655 (SLT), 2006 WL 1307963, at *8 (E.D.N.Y. May 11, 2006) (alteration in original)); *United States v. Sandoval*, No. CR 04-2362 JB, 2006 WL 4079018, at *2 (D. N.M. Jun. 8, 2006) (finding that information a defendant sought was "not material under rule 16, but rather

appear[ed] to be an attempt at a fishing expedition to find material that might lead to some cross-examination at trial").

Brady v. Maryland, 373 U.S. 83 (1963) requires that under the Due Process Clause, the government shall disclose "evidence favorable to an accused upon request…where the evidence is material either to guilt or to punishment." *Caro*, 597 F.3d at 619. Materiality depends on a "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *Id*. In the Fourth Circuit, a reasonable probability must be "sufficient to undermine confidence in the outcome." *Id*. *Brady* is not in place to be used as a discovery device. *Id*. When a defendant can only guess as to what requested materials may expose, it does not satisfy *Brady*'s requirement that the evidence be favorable to the defendant. *Id*. To determine materiality, a court must determine if the evidence withheld from the defense "reasonably could be considered as placing the entire case in such a different light that confidence in the verdict is undermined." *Waters v. Clarke*, 2012 U.S. Dist. LEXIS 140762 *17 (E.D.Va. 2012).

The defendant seeks a copy of the NIT programming code for three stated reasons: (1) "so that [his] computer forensics expert can independently determine the full extent of the information the government seized from [his] computer when it deployed the NIT," (2) "whether the NIT interfered with or compromised any data or computer functions," and (3) "whether the government's representations about how the NIT works are complete and accurate." Def.'s Mot. to Compel at 1. He contends that the information is relevant to his First and Second Motions to Suppress, yet does not explain why the discovery he seeks will help him answer any of the questions he claims, in those motions and the instant motion, must be answered. *Id*. He presents no factual information whatsoever in support of his speculative assertions and fails to show

materiality regarding any of the specified reasons for the seeking the requested information. Indeed, the information sought by the instant motion is not relevant to any of the suppression motions already denied by the Court.[2] The latter motions challenged the sufficiency and legality of the search warrant.

For all of the reasons set forth below, the defendant has also failed to show the materiality to his defense of the information he seeks. Accordingly, to the extent the Court excuses the defendant's failure to timely file the instant motion, it should nevertheless deny it.

A. The defense does not accurately apply the materiality standard for the purposes of Fed. R. Crim. P. 16.

DARBY's interpretation of the materiality standard is broad and incorrect in light of Fourth Circuit precedent. As noted above, the Fourth Circuit's standard for materiality is that, "evidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *Caro*, 597 F.3d at 621. However, DARBY directs the court's attention to a similar case currently being litigated in the United States District Court for the Western District of Washington at Tacoma, where the judge found that the defense had shown that the NIT source code was material to preparing the defense. Def. Mot. to Compel Disc. p. 3. In the Ninth Circuit, evidence is "material" under Rule 16 if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). A defendant must make a "threshold showing of materiality" in order to compel discovery

[2] The motions to suppress challenge the sufficiency and legality of the search warrant (and in a very limited sense, the execution of the warrant). This latter question concerns only whether the triggering condition—logging in to Playpen—occurred. Neither of the defendant's motions challenge the extent of the information identified by the NIT or the NIT's technical aspects, operation, or functionality—either generally or with respect to the defendant, specifically. Accordingly, the NIT source code and an independent forensic analysis of the same are neither relevant nor necessary to the Court's determination of the pending motions.

pursuant to Rule 16(a)(1)(E). *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 government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990).

Although the defense asserts that the *Michaud* court found materiality, the different standards between the circuits warrant a different outcome in DARBY's case.[3] The Fourth Circuit's requirement that there is a "strong indication that [the material] will play an important role" in the defense is narrower than the Ninth Circuit's condition that the defendant show a "possible defense." For the reasons stated above, DARBY is initiating a fishing expedition in which he seeks to obtain information that he either already has access to through the computer instructions or has alternative means of obtaining on his own. While this may satisfy the "possible defense" standard in the Ninth Circuit, the information already made available to him during discovery clearly precludes him from arguing that the entire NIT source code is material in the Fourth Circuit.

DARBY's reliance on the case out of the Ninth Circuit is flawed because the standard is different in the Fourth Circuit. The materiality standard to be applied in his case does not encompass anything that might help his defense. As discussed *infra*, the defendant has not shown a strong indication that the evidence will play an important role in finding evidence, helping witnesses, corroborating testimony, or aiding in impeachment or rebuttal.

[3] Following a government motion to reconsider its discovery order in *Michaud* and review of *ex parte, in camera* materials submitted by the government, that court determined that the government was not required to turn over the further information pertaining to the NIT that DARBY now requests. *United States v. Jay Michaud*, No. 15-cr-5351, ECF 205 (W.D. Wa. May 18, 2016). That court did not reconsider its finding of materiality, however, and later entered an order excluding the NIT evidence and its fruits. *Id.*, ECF 212.

B. Additional discovery to what the government has already provided or offered to provide will not shed light on the accuracy of the identifying data that connects DARBY to both the "Neoumbrella" account and specific activity on the Playpen website.

DARBY contends that, pursuant to Rule 16, he is entitled to the NIT source code because such information may reveal the accuracy of the data the government used to identify DARBY on the Playpen Website. For DARBY to obtain such information, he would have to show that disclosure would "alter the quantum of proof in his favor." *See Caro*, 597 F.3d 608, 621. In other words, DARBY bears the burden of showing that the information he seeks will raise doubt that the NIT accurately identified him as the individual accessing and downloading child pornography. The government will provide DARBY with the computer instructions that generated the identifying data, and the identifying data, additional requests fall outside the scope of appropriate discovery outlined in *Brady*.[4] *See id*. (citing *Brady* and stating that materiality depends on whether the result of the proceeding would be different after disclosing the information to the defendant); *see also White*, 450 F.2d at 268 (deeming requests outside the scope of appropriate discovery as prohibited fishing expeditions). Therefore, additional

[4] In *Michaud*, the defense similarly moved to compel production of the NIT programming code and the government opposed disclosure, as it does here. Prior to the hearing on that motion, the government offered—without conceding any obligation to do so—to make available for review at an FBI facility, the instructions sent to and executed on Michaud's computer, which produced the NIT results. *See* Gov't Resp. to Def.'s Mot. to Compel at 4, *Michaud*, 3:15cr05351, ECF 134 (W.D. Wash. Jan. 21, 2016). The defense agreed and information was provided to the defense pursuant to a protective order, including a copy of the computer instructions sent to Michaud's computer that, when executed, produced the NIT results, the NIT results themselves, the date and time the NIT was executed on Michaud's computer, and the Playpen thread that Michaud was accessing when the NIT was executed. *Id*. at 1, 4. Without conceding any obligation to do the same in light of the defendant's untimely request and his similar failure to show materiality, the government is willing to make the same information available to the defendant in this case. The government strenuously opposes disclosure of any additional information described in Tsyrklevich's declaration, as it has consistently done in *Michaud*.

discovery requests regarding the government's chain of custody of the NIT are cumulative and unnecessary.

First, DARBY's fundamental misunderstanding of the NIT's basic structure misinforms his perception of how the NIT processed and transmitted the data that identified him as a Playpen user. Relying on the Tsyrklevich declaration, DARBY asserts that the NIT is comprised of four components, all of which he claims are necessary to determine the accuracy of the identifying information. *See* Decl. of Tsyrklevich (hereinafter, "Tsyrklevich Decl.") ¶ 4. Of the alleged four components, he claims there is an "exploit," a "payload," software that generates the payload and injects a unique identifier into it, and a server that stores the delivered information. *Id*. In reality, the NIT is one component, which is the computer instructions delivered to DARBY's computer that gathered his identifying information after he logged into the Playpen website. Ex. A, Decl. of Special Agent Daniel Alfin hereinafter, "Alfin Decl.") ¶ 5[5]. As noted before, those instructions, and the information obtained via their execution, will be made available for review. *Id*.

Particularly, DARBY seeks disclosure of the "exploit" in order to determine whether the government "executed additional functions outside the scope of the NIT warrant." Tsyrklevich Decl. p. 3. However, even assuming that the NIT does have multiple components, the "exploit" is not relevant to anything found in the warrant; it would only show how the NIT was deployed to DARBY's computer, not what it did once it began interacting with his computer. Alfin Decl. ¶ 12. Furthermore, the defense's contention that the "exploit" could have made changes to DARBY's computer is purely theoretical. Alfin Decl. ¶ 14. While it is possible for some

[5] While Special Agent Alfin's declaration was originally drafted for the related case, *United States v. Matish*, 4:16cr16, pending before Senior United States District Judge Henry Coke Morgan, the same information applies in this case.

exploits to do so, the NIT in question and the exploit it used to deliver computer instructions did not do so. *Id*. The defense experts point to no evidence that the NIT initiated any changes to DARBY's computer system or security firewall that would warrant concern that the identifiers misidentified DARBY as a Playpen user. *Id*. To alleviate DARBY's concerns about the "exploit," the government will offer to allow the defense to review the two-way network data stream transmitted to the FBI from DARBY's computer after the NIT's deployment. Alfin Decl. ¶ 15. Reviewing the data stream would show the defense that the data sent from DARBY's computer is identical to the data the government provided as part of discovery. Alfin Decl. ¶ 16.

Additionally, DARBY requests the "server component," but this is unnecessary because there are alternative means of verifying the accuracy of the NIT information. Alfin Decl. ¶ 18. The government agrees to provide a copy of the data stream sent by DARBY's computer to the government as a result of the NIT, so defense experts do not need to access government servers at all. Alfin Decl. ¶ 19. Once the copy is provided to the defense, the defense expert can compare the information sent to the government by the NIT to the information provided in discovery to determine whether the material the government recorded from DARBY's computer is in fact what was sent by DARBY's computer. *Id*. The government has confirmed that the information sent to the government from DARBY's computer is exactly what the government will disclose in discovery as obtained by the NIT. *Id*.

Lastly, DARBY demands the computer code that "generates the payload and injects an identifier" in order to contest the legitimacy and uniqueness of the identifier used to find him. Tsyrklevich Decl. p. 3. However, this is unnecessary information because a unique identifier is incorporated into the NIT upon each deployment. When the user's computer activates the NIT and sends information to the government, the unique identifier accompanies the information.

Alfin Decl. ¶ 26. DARBY's speculation concerning the existence of duplicate unique identifiers and the accuracy of the NIT information is unfounded, because all identifiers received by the government matched those that the government generated without any duplicates. Alfin Decl. ¶ 26. In fact, a review of the FBI database containing the information gathered by the NIT revealed that: (1) there are no duplicate unique identifiers within the database, so each identifier assigned to each Playpen user was unique, (2) the identifier associated with "Neoumbrella" was unique, and (3) only identifiers generated by the NIT were in the database, which means that no outside entity tampered with the identifiers used in the Playpen investigation. Alfin Decl. ¶ 27.

The defendant has not proven that disclosure would alter the quantum of proof in his favor and therefore has not proven that any further information is material to his defense. The information he seeks will not raise any suspicion that the NIT did not accurately identify him as the person accessing child pornography. The government provided the defendant with identifying data and everything he needs to answer his questions regarding accuracy and identification. Additional discovery requests do not assist him in his pursuit of these questions, and therefore his motion to compel should be denied.

B. The requested discovery also has no bearing on DARBY's claim that someone or something else may have been responsible for the downloading of child pornography on his device.

DARBY speculates about the possibility that the NIT disabled DARBY's computer security, and, accordingly, argues the possibility that different users could be linked to each other's actions. Tsyrklevich Decl. ¶ 6. To obtain the source code and subsequently present to the jury that the child pornography came from some other source, DARBY must show that the requested discovery holds a "reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *Caro*, 597 F.3d at 619. This

would be a difficult argument considering DARBY's confession to collecting child pornography. And, if DARBY is only guessing as to what the materials may provide, then *Brady*'s requirement that the material must be favorable to the defendant is not satisfied. *Id*. at 619. In DARBY's case, the entire source code is not material to his defense because the evidence does not indicate the possibility that DARBY unknowingly obtained child pornography.

To be malware, a software or computer program must set out to make "malicious" changes to a computer's security settings or systems. The NIT did not deploy any program that would have made changes to DARBY's computer; it merely interacted with his computer to obtain the information that traced him to the "Neoumbrella" account. Alfin Decl. ¶ 6. Further, after the NIT sent instructions to DARBY's computer, it ceased interaction and left no residual openings that would allow the government to return for further access to that computer. Alfin Decl. ¶ 8. Outside of pure speculation regarding a theoretical possibility, DARBY points to no facts to suggest otherwise.

Should the defense decide to further inquire about any potential malware that could have been left on DARBY's computer, his devices are available for review. Alfin Decl. ¶ 35. However, the defense not reviewed DARBY's devices nor the network data, which would be a valuable tool for searching for malware. Alfin Decl. ¶ 32. Alternative to inspecting the source code itself, there are other ways to find malware on a device that would help the defense identify other malware that may have led to the unintentional downloading of child pornography. Alfin Decl. ¶ 33 and 34. For example, an investigator may find all files and programs with unknown purpose and find its function to determine whether they are malware. Alfin Decl. ¶ 33. Additionally, the investigator can conduct a dynamic analysis on devices suspected of containing malware by creating copies of all suspect files and executing them in test environments to

determine their functions. Alfin Decl. ¶ 34. DARBY's devices, as available to the defense, are appropriate subjects for both malware-testing techniques described above. Alfin Decl. ¶ 35. Therefore, the defense does not need the source code to determine whether malware was responsible for the collection of child pornography found on DARBY's computer rather than DARBY himself.

The defendant has not shown that the discovery he requests holds a reasonable probability that if it were to be disclosed, the results of the proceeding would be different. DARBY only speculates so to what the materials might reveal, and thus *Brady*'s requirement that the material in fact be favorable to him is not satisfied. Because the defendant has not met the requirements for further discovery, his motion to compel should be denied.

C. The extent of the information seized from the defendant's computer

As explained in the NIT search warrant affidavit and as the government has disclosed, the NIT programming code consists of computer instructions that caused a user's activating computer to deliver certain authorized information to a computer controlled by the government. *E.g.*, Gov't Resp. to Def.'s First Mot. to Supp., Ex. A at 24-26, ¶¶ 33-34. Review of the programming code is unnecessary to determine the extent of information seized from the defendant's computer by operation of the NIT because the information collected by the NIT is available to the defense, and that information answers this question. It includes the defendant's IP address, a unique identifier generated by the NIT to distinguish the data from other computers, information about whether the NIT had already been delivered to the computer, and the computer's operating system, "Host Name," active operating system username, and Media Access Control ("MAC") address. That information is contained in the "user report" available to

the defendant, should the defendant contact the government to view the information as offered. The collection of all such information was authorized by the NIT warrant.

The defendant fails to provide any factual support regarding what other information he suggests might have been collected through the NIT, let alone other information that was collected.[6] Indeed, the defendant has not even asked the government whether any information was collected by the NIT beyond that described in the warrant and reflected in the user report. The answer is no. Regardless, even if the NIT had collected further information, only that information could be subject to suppression as outside the scope of the warrant—not the information specifically authorized by that warrant. Because, however, there is no such further information, there is nothing to suppress and no compelling need for an expert to independently determine the information obtained via the NIT.

The defendant also fails to provide any information to this Court to meet his burden of showing why or how review of the programming code, as opposed to reviewing the information collected by the NIT (or other information the government could provide) would answer any question about what information the NIT collected. Indeed, the defendant has not asked for any

[6] Nothing in the defendant's motion or the witness declaration he attaches claims, for example, that the computer instructions would have collected information other than what the government disclosed they did. Nor does he even identify what supposed other information might have been collected. Rather, the declaration's author posits, after having reviewed the computer instructions comprising the NIT, "whether the payload that has been provided was the only payload associated with the NIT or whether other payloads were executed" and claims that he needs to analyze and understand additional information to determine whether the information provided in discovery "was the only component executing and reporting information to the government" and/or "whether [that additional information] executed additional functions outside the scope of the NIT warrant." Tsyrklevich Decl. at 3. This speculation is wholly irrelevant to the matter at hand. The results provided to the defendant consist of the only information collected by the NIT. Even if some unspecified additional information had been collected by the NIT (or some other set of computer instructions), the defendant does not claim that this unspecified information bears on this case. Nor could he, because the only NIT information relied on by the government in the warrant for the defendant's home and that it may rely on at trial is that which has already been disclosed.

information related to the use of the NIT and the information it collected, beyond that already offered by the government, which might have enabled him to assess the questions he now claims compel production of the NIT programming code. Accordingly, he fails to show how review of the programming code would reveal "the full extent of the information the government seized from DARBY's computer" – particularly in light of the fact that the information collected by the NIT has already been disclosed. The defendant therefore fails to make any showing of materiality or to present facts that tend to show the government is in possession of information helpful to the defense.

D. Whether the NIT interfered with or compromised any data or computer functions

Review of the programming code is also not material for the purpose of determining whether the NIT interfered with or compromised any data or computer functions. The defendant presents no information to support this wholly speculative hypothesis. Nor can he. The defendant has not made any discovery requests for information concerning the operation of the NIT beyond the information already offered by the government, other than his request for the NIT programming code and the NIT results. In the instant motion, he fails to provide any information regarding what he means by "interfer[ing] with or compromis[ing] any data or computer functions." Def.'s Mot. to Compel Disc. at 1. He also does not explain how, if such interfering with or compromise of data or computer functions did occur—and it did not—this fact would lead to suppression of any evidence, since the only evidence "seized" was authorized by the warrant. Nor has the defendant made any showing of how review of the programming code would provide information to support an argument for some other sort of relief if the NIT did interfere with or compromise any data or computer functions. Finally, he has not shown the impact of any such interference or compromise on any defense to the charges pending against

him. Indeed, he cannot do so, because, as the government has disclosed, the conduct on which the indictment is based relates to the defendant's activities on the Internet that were discovered on the defendant's computer media found at his residence (and that he confessed to during an interview with law enforcement).

Critically, the defendant has ongoing access to the forensic examination conducted of his computer and other digital devices seized. He has also been provided with substantial information pertaining to his dates of access to the pertinent website, and the date and time at which the NIT identified his IP address accessing the site. Despite having that information, he presents nothing to this Court from any examination of his devices to support his rank speculation that the NIT could have interfered with or compromised any data or computer functions, let alone that it did. Nor has the defendant ever asked to perform an independent forensic examination of his computer or other digital devices. Absent some indication—based in fact as opposed to speculation and conjecture—that the NIT interfered with or compromised any data or computer functions—something the government disputes occurred—the defendant fails to present any facts tending to show that the government possesses information that "would . . . actually help[] prove his defense." *Caro*, 597 F.3d at 621.

E. Whether the government's representations about how the NIT works in its warrant applications were complete and accurate

Review of the programming code is also not material for the purpose of determining whether representations about how the NIT works are complete and accurate. By its nature, this is an entirely speculative request that any defendant could make, at any time, in any case, in an effort to justify any request for information from the government. The defendant presents no facts to suggest that the government is in possession of any information helpful to the defense on that issue. Nor does he even claim that the NIT worked other than as described, just that he

needs to verify that its actual operation comported with that description. Such rank speculation cannot support a finding of materiality. *Caro*, 597 F.3d at 621. In fact, this sort of speculative request turns the criminal discovery process on its head. If the standard for obtaining criminal discovery were, "What if the government's representations were not correct or complete," then there would be no limitation to criminal discovery and every defendant would be entitled to fish through every scrap of information in the government's possession in order to look for something that might impeach a government representation. That is inconsistent with the disclosure requirements established by Rule 16, *Brady*, and *Giglio*.

With respect, specifically, to the descriptions of the NIT set forth in the search warrant affidavit,[7] the defendant has not identified any facts to suggest that those descriptions, in particular, are incomplete or inaccurate, despite having received substantial information pertaining to the use and execution of the NIT warrant on his computer, specifically—including exactly where on the website he was (a posting thread in the kinky fetish – zoo subforum) when he received the NIT. He also has access to the forensic examination of the devices seized from his home and has not requested to conduct any independent examination of those devices. Even having all of this, the best the defendant can do is hypothesize that the NIT could have worked other than as described. He cannot even muster an explanation as to what, if any, description of the NIT he is unable to test. A defendant can always allege, absent factual support, that it is arguably possible that the government did not include complete and accurate information in a search warrant. A mere allegation simply will not supply a basis for seeking to rummage

[7] In describing how the NIT would operate, the NIT affidavit explained that when a user's computer accessed Playpen and downloaded its content in order to display web pages on the user's computer, that content would be augmented with additional computer instructions (which comprised the NIT) that, once downloaded to a user's computer would cause the user's computer to transmit the information specified in the warrant. Gov't Resp. to Def.'s First Mot. to Supp., Ex. A, at 24, ¶ 33.

through the government's files. *See Caro*, 597 F.3d at 621. Indeed, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion" to require discovery on this point, and for the Court to ignore that requirement, as the defendant wishes it to do, "is to abuse its discretion." *Mandel*, 914 F.2d at 1219.

The defendant makes no showing as to how the NIT programming code, as opposed to other information that has been or could be made available, would actually further his defense. Rather he merely speculates that such a review might produce information that could impeach the NIT warrant or testimony concerning the process by which he was identified. "Mere speculation that *Brady* material exists does not justify fishing expeditions in government files." *United States v. Paulino*, 1996 U.S. App. LEXIS 30032, at *4 (4th Cir. Nov. 20, 2006); *see also United States v. Crowell*, 586 F.2d 1020, 1029 (4th Cir. 1978); *United States v. Brown*, 360 F.3d 828, 833 (8th Cir. 2004) ("[M]ere speculation that materials may contain exculpatory evidence is not . . . sufficient to sustain a *Brady* claim); *United States v. American Radiator & Standard Sanitary Corp*., 433 F.2d 174, 202 (3d Cir. 1970) ("[A]ppellants' mere speculation about materials in the government's files [does not require] the district court or this court under *Brady* to make the materials available for their inspection."). Absent the required factual showing, the defendant's request amounts to nothing more than a fishing expedition, which is not sanctioned by Rule 16 or any other law.

The defendant contends that the government's disclosure of information in other cases is relevant to the inquiry in this case. First, the defendant points to one related case in which a court *initially* ordered the government to disclose information related to the NIT programming code. Def.'s Mot. to Compel Disc. at 3 (citing Order Granting Third Mot. to Compel Disc., *United States v. Michaud*, Crim. No. 3:15cr05351, ECF 161 (W.D. Wash. Feb. 17, 2016)). In

that case, the government—as it does here—vigorously objected to disclosure of the NIT programming code; litigation concerning such disclosure is ongoing. *See* Minute Entry for Proceedings, *Michaud*, Crim. No. 3:15cr05351, ECF 199 (W.D. Wash. May 12, 2016). Defendant fails to note that, as discussed *supra*, after the government moved for reconsideration of the court's order and an *in camera*, *ex parte* hearing, the court reversed its earlier ruling and declared that the government was not required to produce the requested discovery concerning the NIT programming code, including the items described in Vlad Tsyrklevich's Jan. 13, 2016 Declaration. Nothing about the government's conduct in that litigation is inconsistent with the position the government has taken in this case.

The defendant also contends that the government's disclosure of information pertaining to a different network investigative technique in an unrelated case is inconsistent with the government's position concerning the disclosure of the NIT in this case. It is not. The *Cottom* case in the District of Nebraska, No. 13-cr-108, involves a different investigation of a different website using a different investigative technique than the one pertinent to the defendant's case. That investigative technique was publicly sourced and no longer in use—in fact, example programming code for the technique was available for review on a public website. After the completion of suppression hearings and before trial, the government disclosed, in an expert notice, information about government expert witnesses, including details about the specific investigative technique used in that case, about which those experts were to testify at trial. The government did not, in that case, as it does here, challenge whether defendants had met their burden to demonstrate materiality related to the disclosed information. Further, there—unlike here—the government did not assert that the particular technique was subject to law enforcement privilege, see infra, as that technique was publicly available.

Although the defendant sets forth three purposes for which he seeks disclosure of the NIT programming code, he fails to identify any facts that he claims establish the materiality of that information to his suppression motions or to his defense. Nor has the defendant shown that the government's objection to disclosure is inconsistent with its conduct in other cases.

II. None of the Defendant's Other Claims of Relevance Establish Materiality

The defendant suggests that review of the NIT programming code is necessary to "investigate the chain of custody for data collected remotely by the NIT." Def.'s Mot. to Compel Disc. at 2. This request is again purely speculative—he presents no facts whatsoever to suggest that there are or were any issues with the so call "digital 'chain of custody'" pertaining to the NIT-derived information. That the NIT-derived information is computer-related information does not entitle the defendant or his expert to rummage through government files—digital or otherwise—in the hope of finding an error in the chain of custody. *Cf. United States v. Guzman-Padilla*, 573 F.3d 865, 890 (9th Cir. 2009) ("[M]ere speculation about materials in the government's files [does not require] the district court . . . under *Brady* to make the materials available for [appellants'] inspection."); *Am. Radiator & Standard Sanitary Corp*., 433 F.2d at 202 (same).

III. The NIT Programming Code is Subject to Qualified Law Enforcement Privilege

If the Court finds—as it should—that the defendant has failed to meet his burden to show that the requested information is material and otherwise discoverable under Rule 16, that will resolve the defendant's motion. In the event the Court were to determine that the NIT programming code is material to DARBY's defense, however, then the requested information pertaining to that code is nevertheless subject to a qualified law enforcement privilege, as its

disclosure would be harmful to the public interest.[8] Specifically, disclosure could diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations, and possibly lead to other harmful consequences not suitable for inclusion in this response. Ex. B, Affidavit of Robert Stone (filed under seal) (hereinafter Stone Aff.) [9] ¶5. As explained below, courts have generally recognized that, because of the sensitivity of information that may support this type of privilege claim, it is appropriate to consider a submission from the government *ex parte* and *in camera*. Accordingly, in the event it determines the defendant's request for programming code is material, the United States accordingly requests that the Court permit the United States to offer evidence in support of its privilege claim *ex parte* and *in camera*.[10]

The privilege has its roots in *United States v. Roviaro*, where the Supreme Court first recognized a qualified "informer's privilege" that protects the identity of government informants. 353 U.S. 53, 59 (1957). Courts have since extended the qualified privilege in *Roviaro* to cover other investigative techniques, including traditional and electronic surveillance. For example, in

---

[8] Further, the FBI has derivatively classified portions of the tool, the exploits used in connection with the tool, and some of the operational aspects of the tool in accordance with the FBI's National Security Information Classification Guide. As of the date of this filing, the government is waiting on a formal, signed document from an FBI Original Classification Authority to detail the specific aspects of the classification of the information.

[9] While the Stone declaration was originally drafted for the related case, *United States v. Matish*, 4:16cr16, pending before Senior United States District Judge Henry Coke Morgan, the same information applies in this case.

[10] Should the Court permit the *ex parte* and *in camera* submission, the government advises that a Classified Information Security Officer with the Litigation Security Group at the U.S. Department of Justice will have to assist in providing certain documents to the Court. Arranging for this may cause a short delay, and the government requests the Court's indulgence in arranging such an event.

United States v. Green, the D.C. Circuit applied the privilege to bar disclosure of the location of an observation post in a drug investigation because failing to do so would "likely destroy the future value of that location for police surveillance." 670 F.2d 1148, 1155 (D.C. Cir. 1981). In *United States v. Van Horn*, the Eleventh Circuit applied the privilege to bar disclosure of the nature and location of electronic surveillance equipment because disclosure would "educate criminals regarding how to protect themselves against police surveillance." 789 F.2d 1492, 1507 (11th Cir. 1986); *see also In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010) (finding that the district court erred by failing to apply the privilege to reports made by undercover agents because they contained "detailed information about [] undercover operations," disclosure of which would "hinder [law enforcement's] ability to conduct future undercover investigations"). The purpose of the privilege is, among other things, "to prevent disclosure of law enforcement techniques and procedures." *In re Dep't of Investigation*, 856 F.2d 481, 484 (2d Cir. 1988); *Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007).

The government bears the initial burden of showing that the law enforcement privileges applies to the materials at issue, *In re The City of New York*, 607 F.3d at 944, and the courts then apply a balancing test in determining whether disclosure is required, *Van Horn*, 789 F.2d at 1508. To meet its initial burden, the government must show that the materials contain information that the law enforcement privilege is intended to protect, which includes "information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witnesses and law enforcement personnel [or] the privacy of individuals involved in an investigation, and information that would otherwise . . . interfere[] with an investigation." *In re The City of New York*, 607 F.3d at 944 (citations and internal quotation marks omitted); *see also Commonwealth*

of Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007) (extending privilege recognized for "confidential government surveillance information" to "law enforcement techniques and procedures"). *See* Stone Aff. ¶ 6.

Because the evidence required to establish the privilege is often sensitive, courts have recognized that it is appropriate to permit the government to make its showing through an *ex parte* and *in camera* evidentiary hearing, the record of which should be sealed for later review. *See, e.g.*, *United States v. Johns*, 948 F.2d 599 (9th Cir. 1991) (approving, over the defense objection, court's consideration of the government's request to maintain the confidentiality of an informant in an *ex parte, in camera* hearing); *United States v. McLaughlin*, 525 F.2d 517, 519 (9th Cir. 1975) (upholding trial court's conducting of *in camera* hearing regarding disclosure of informant's identity and determining that disclosure was not required); *United States v. Fixen*, 780 F.2d 1434, 1439-40 (9th Cir. 1986) (suggesting use of *in camera* proceedings to resolve law enforcement privilege issues); *United States v. Kiser*, 716 F.2d 1268, 1273 (9th Cir. 1983) (remanding to district court to conduct *ex parte, in camera* hearing pertaining to *Roviaro* privilege issue and citing cases authorizing *in camera* hearings in similar situations); *Van Horn*, 789 F.2d at 1508 (district court held *in camera* hearing); *Global Relief Found, Inc. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002) ("*Ex parte* consideration is common in criminal cases where, say, the identity of information might otherwise be revealed"); *In re Department of Homeland Security*, 459 F.3d 565, 569-71 (5th Cir. 2006) (instructing the district court in a civil case to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies"); *In re The City of New York*, 607 F.3d at 949 (determining requesting party did not have compelling need for requested information based on *in camera* review of the documents); *Rigmaiden*, 844 F. Supp. 2d at 982 (denying defendant's requests for discovery concerning

investigative technique after *ex parte, in camera* review at which the court heard the government's reasons for nondisclosure); *cf. In re Grand Jury Proceedings #5 Empanelled Jan. 28, 2004*, 401 F.3d 247, 253 (4th Cir. 2005) (approving the use of *ex parte* and *in camera* review of allegedly privileged documents in the context of a crime-fraud exception claim).

At an *ex parte in camera* hearing, the United States can provide a more detailed presentation about both the nature of the information that the defendant is requesting and the government's concerns regarding its disclosure. Because of the sensitivity of the technique and for other reasons, simply filing the material under seal with a protective order is inadequate to address the government's concerns. Indeed, courts have recognized that sealing documents and materials containing such sensitive information is frequently inadequate to prevent its public disclosure. *See, e.g., In re The City of New York*, 607 F.3d at 937-39 (citing numerous specific examples of instances where "sealed" materials were inadvertently or intentionally disclosed, and concluding that "[i]n light of how often there are all-too-human lapses with material filed 'under seal'" that it could not "conclude with confidence that filing" the sensitive information would adequately protect the information from public disclosure).

Upon a finding that the privilege applies, there is a "pretty strong presumption against lifting the privilege." *In re The City of New York*, 607 F.3d at 945 (*quoting Dellwood Farms v. Cargill*, 128 F.3d 1122, 1125 (7th Cir. 1997)). The burden shifts to the defendant, who must show that his need for the information overcomes the public interest in keeping it secret. *See Alvarez*, 472 F.2d at 113 (finding, regarding disclosure of informer identity, that "in balancing the interest of the government against that of the accused, the burden of proof is on the defendant to show the need for disclosure); *see also Van Horn*, 789 F.2d at 1507. The public interest in keeping the information private must be balanced against a defendant's articulated need for the

information. *See Roviaro*, 353 U.S. at 628-29. "Whether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [privileged information], and other relevant factors." *Id*. at 629.

In conducting this balancing, the court should consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982); *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (the question is "whether the [defendant] demonstrate[s] an authentic 'necessity,' given the circumstances to overbear the qualified privilege); *United States v. Foster*, 986 F.2d 541, 543 (D.C. Cir. 1993) (balancing the defendant's need for information against importance of government's interest in avoiding disclosure).

In striking this balance, the Court should also keep in mind that the need for disclosure is more limited in the context of a suppression hearing than at trial. *See McCray v. Illinois*, 386 U.S. 300, 311 (1967); *see also Rigmaiden*, 844 F. Supp. 2d at 990 (applying *McCray* in the context of motion for disclosure of electronic tracking equipment). Even if the party seeking disclosure successfully rebuts the presumption (by a showing of, among other things, a "compelling need"), the court must still then weigh the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. *In re the City of New York*, 607 F.3d at 948.

As can be explained in more concrete terms in an *ex parte, in camera* hearing, the public interest in nondisclosure here significantly outweighs the defendant's need for the information,

particularly in light of the defendant's speculative claims regarding the materiality of the requested information. In particular, the risk of circumvention of an investigative technique if information is released has been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See Van Horn*, 789 F.2d at 1508.[11] Accordingly, in the event the Court finds the requested information to be material, the Court should hold an *ex parte, in camera* hearing to assess the applicability of the privileges and the defendant's need for the materials.

The analysis of the Sixth Circuit in *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015) is instructive here. *Pirosko* affirmed the district court's denial of a motion to compel disclosure of "the law enforcement tools and records" (there, ShareazaLE, a proprietary program used exclusively by law enforcement) used to search a defendant's computer for child pornography. 787 F.3d at 362. Similar to this case, the defendant in that case presented a purported expert declaration claiming that analysis of the government's investigative tools "can determine whether law enforcement officers manipulated data on the subject computer [or] the error rates in records used." *Id*. at 363. The defendant also contended that review of the source code was necessary to allow "his experts to determine whether [the software] gives government officials 'the ability to manipulate settings or data on the target computer (even unintentionally),' 'whether the software allows agents to override shared settings to download files that a normal user would not be able to download,' and 'the error rate' associated with the software." *Id*. at 365. As here, the defendant produced no evidence to suggest that any of those speculative

[11] Risk of circumvention has also been accepted by numerous courts as a basis for nondisclosure in the civil FOIA context. *See, e.g., James v. U.S. Customs and Border Protection*, 549 F. Supp. 2d 1, 10 (D.D.C. 2008) (concluding that CBP properly withheld information under FOIA that "could enable [others] to employ measures to neutralize those techniques"); *Judicial Watch v. U.S. Department of Commerce*, 337 F. Supp. 2d 146, 181-82 (D.D.C. 2004) ("[E]ven commonly known procedures may be protected from disclosure if the disclosure if the disclosure could reduce or nullify their effectiveness.")

concerns were actually manifested – such as, through an examination of the defendant's computers. The government objected to disclosure on both Rule 16 materiality and law enforcement privilege grounds, arguing that granting the motion to compel "would compromise the integrity of its surveillance system and would frustrate future surveillance efforts." *Id*. at 365. The Court of Appeals for the Sixth Circuit endorsed the government's argument on both points, holding that "it is important for the defendant to produce some evidence of government wrongdoing" – which that defendant had failed to do – when balancing the government's assertion of the law enforcement privilege against the needs articulated by a defendant. Id. at 365-66 (emphasis supplied).

Similarly persuasive is the District Court' analysis in *United States v. Rigmaiden*. In that case, the government, acting on the authority of a tracking device warrant, used a cellular site simulator in order to locate a wireless "aircard" that assisted in locating and ultimately identifying the defendant. [12] The defendant moved to compel production of additional information pertaining to the technology, methods, and personnel involved in tracking the "aircard." The government provided information pertaining to the aircard tracking, but opposed disclosure of technical details, asserting law enforcement privilege. Following hearings related to the issues, the Court denied the defendant's requests, finding either they were speculative and accordingly, not material, or that the defendant had not demonstrated a compelling need in light of the government's persuasive showing regarding the law enforcement privilege. *Rigmaiden*, 844 F. Supp. 2d at 996-1004.

Here, the defendant cannot demonstrate any compelling need for the requested information. As demonstrated above, his requests are entirely speculative and conclusory. Such

[12] An "aircard" may be attached to a laptop in order to provide Internet service.

requests are insufficient to justify a compelling need, in light of the government's assertion of privilege. *See United States v. Buras*, 633 F.2d 13566, 1360 (9th Cir. 1980); *Guzman-Padilla*, 573 F.3d at 890. The defendant cannot compel disclosure based simply on his conjecture that privileged material may contain something relevant.

In addition, the defendant has been provided or has access through discovery to "adequate alternative means of getting at the same point" to which he claims disclosure of the information is relevant. *Harley*, 682 F.2d at 1020. The government is willing to provide, as it did in *Michaud*, the computer instructions comprising the NIT that, when executed, produced the NIT results. Those results have already been disclosed. This information would allow him to verify that the particular instructions would have produced the particular results and therefore that the NIT was properly described and operated consistent with that description. He also has a copy of the forensic report of his computer and substantial information pertaining to his dates of access to the pertinent site and the date and time at which the NIT identified his IP address accessing that site. He may analyze that information if he wishes to verify that the NIT did not interfere with or compromise any data or computer functions. And, to the extent the defendant wishes to request chain of custody documentation from the government regarding items to be admitted at trial, there are numerous avenues available for him to request such information short of seeking to rummage through the government's files or to compel the government to disclose privileged material. To date, he has not sought any such information. Accordingly, the defendant cannot establish the sort of compelling need required to outweigh the significant public interest in nondisclosure of additional materials pertaining to the use and execution of the court-authorized NIT.

CONCLUSION

For the foregoing reasons, the defendant's motion to compel should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By:_____/s/_____
Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov

Leslie Fisher
Trial Attorney
U.S. Department of Justice
Criminal Division
Child Exploitation & Obscenity Section
1400 New York Ave. NW, Suite 600
Washington, D.C. 20005
Office: (202) 616-2557
Fax: (202) 514-1793
Leslie.fisher2@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 16th day of June, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Richard Colgan, Esq.
Rodolfo Cejas, Esq.
Assistant Federal Public Defender

_____/s/_____

Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov