

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

Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 4:16cr16
	)	
EDWARD JOSEPH MATISH III,	)	
	)	
Defendant.	)	

GOVERNMENT’S SURREPLY TO DEFENDANT’S MOTION TO COMPEL DISCOVERY

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Eric M. Hurt, Assistant United States Attorneys, and submits its surreply to the defendant, EDWARD JOSEPH MATISH III’s Motion to Compel Discovery. For the reasons set forth below, the defendant’s motion should be denied.

**INTRODUCTION**

Defendant EDWARD JOSEPH MATISH III (“the defendant”) is charged in this case with accessing with intent to view child pornography involving a prepubescent minor and receipt 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 identify 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 a 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. Further information on the NIT can be found in previous motions filed by the Government.

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 (ECF No. 37). His request to compel disclosure of this information represents nothing more than a fishing expedition for information that either is not material to his defense or has already been provided. The defendant does not meet the 4th Circuit standard for materiality and incorrectly relies on the 9th Circuit standard in his materiality claim. Moreover, the NIT programming code is protected by a qualified law enforcement privilege. Accordingly this Court should deny the defendant’s motion.

**BACKGROUND ON DISCOVERY PERTAINING TO THIS MOTION**

At the arraignment on February 18, 2016, the parties entered into an agreed discovery order. ECF No. 12. The government provided initial discovery pursuant to that order on March 4, 2016. Among the items included in that disclosure were redacted copies of the court authorizations obtained from the United States District Court for the Eastern District of Virginia to (1) monitor the site users’ communications, and (2) use a Network Investigative Technique (“NIT”) on the site, as well as additional materials pertaining to the investigation such as investigative reports, including the forensic report regarding the defendant’s digital devices.

On March 10, 2016, the government provided additional discovery materials responsive to the defendant’s written request made the day before, along with a plea offer letter. On March

15 and 16, 2016, the defendant submitted two additional sets of discovery requests by letter, the first concerned information related to Playpen and its users and the second sought disclosure of the NIT source code. The defendant filed two motions to suppress on March 17, 2016, one of which sought to suppress the information identified by the NIT on a number of different grounds.

The parties held a discovery meeting on March 21, 2016 at the FBI, Peninsula Resident Agency in Newport News that lasted approximately two hours. During that meeting, the parties reviewed extensive discovery related to the “Broden” Playpen user account,<sup>1</sup> including information related to the use of the NIT, the NIT results for that account, and the Playpen thread that the defendant was accessing when the NIT was executed. The parties also reviewed the forensic examination report for the defendant’s computer. During the meeting, defense counsel made a number of additional discovery requests and agreed, in principle, to the entry of a protective order.

During a phone call on March, 23, 2016, the parties discussed, among other topics, the preliminary motions that the defendant had filed on March 17, 2016, and the outstanding discovery requests, including the defendant’s request for the NIT programming code. The government objected to that request. On April 26, 2016, the government responded in writing to the defendant’s April 8 clarification letter and outstanding discovery requests, including the request for the NIT programming code. Regarding that request, the government 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 further advised that it did not believe—and the defendant had failed to indicate why—that information was material to his defense. The government also advised that

---

<sup>1</sup>The “Broden” account is the account associated with the defendant.

the investigative technique is subject to law enforcement privilege, which the government asserted. The government noted that the information collected through the use of the court-authorized NIT had been made available for counsel's review during the March 21, 2016 discovery meeting and would remain available for further review during the pendency of the litigation. The government also offered to provide the defendant a copy of that information subject to the entry of a protective order. Additionally, regarding the NIT results, the government explained that 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, as reflected in the user report that counsel had reviewed on March 21, 2016. The government clarified that 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. 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.

On May 3, 2016, the day after his preliminary motions were due, the defendant asked the government to reconsider its position concerning disclosure of the NIT source code. The defendant stated he was seeking a copy of the NIT programming code so that a computer forensics expert could determine the extent of the information seized from his computer through the NIT; whether the NIT interfered with or compromised any data or computer functions; and whether the government's representations about how the NIT works are complete and accurate. The defendant claimed that this forensic information was relevant to his pending motions and to trial, but did not further explain why he believed them material to his defense. On May 5, 2016,

the government confirmed its previously stated position concerning disclosure of the NIT programming code. The defendant filed his motion to compel the following day. On May 17, 2016, the Government filed a response to defendant's motion to compel discovery. Defendant filed a reply to the Government's response on May 23, 2016. The Government now files a surreply to defendant's reply after requesting permission on May 24, 2016.

### **LAW AND ARGUMENT**

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).

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.* A defendant cannot meet this burden through "general description[s] of the information sought" nor through "conclusory allegations of materiality." *Id.* Moreover, Rule 16 does not authorize a defendant to embark on a fishing expedition, which is exactly what the defense requests amount to. *See United States v. White*, 450 F.2d 264, 268 (5th Cir. 1971).

*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.V.A. 2012).

The defendant seeks a copy of the NIT programming code for two main reasons: (1) the defense wishes to challenge the Government’s chain of custody regarding the connection between Mr. Matish’s computer and the Playpen website; and (2) the defendant claims that the child pornography found on Mr. Matish’s computer came from someone or somewhere else. Def. Reply to Gov. Response to Compel Disc. at 4 and 5. For all of the reasons set forth below, the defendant has failed to show the materiality of the information he seeks for his defense.

**I. As an overarching issue, the Defense does not accurately apply the materiality standard for the purposes of Fed. R. Crim. P. 16.**

Matish’s interpretation of the materiality standard is broad and incorrect in light of 4th Circuit precedent. As noted above, the 4th 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 (emphasis added). However, Matish 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. Reply to Gov. Resp. to Mot. to Compel Disc. p. 5. In the 9th 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 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 clearly found materiality, the different standards between the circuits warrant a different outcome in Matish’s case.<sup>2</sup> The 4th Circuit’s requirement that there is a “strong indication that [the material] will play an important role” in the defense is narrower than the 9th Circuit’s condition that the defendant show a “possible defense.” For the reasons stated above, Matish is initiating a fishing expedition in which he seeks to obtain information that he either already has through the computer instructions or has alternative means of obtaining on his own. While this may satisfy the “possible defense” standard in the 9th 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 4th Circuit.

---

<sup>2</sup> 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 Matish now requests. *United States v. Jay Michaud*, No. 15-cr-5351, Dkt. 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.*, Dkt. 212.

Matish's reliance on the case out of the 9th Circuit is flawed because the standard is different in the 4th Circuit. The materiality standard to be applied in his case does not encompass anything that might help his defense. 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. Therefore, Matish's motion requesting discovery production should be denied.

**II. Additional discovery to what the Government has already provided will not shed light on the accuracy of the identifying data that connects Matish to both the "Broden" account and specific activity on the Playpen website.**

Matish 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 Matish on the Playpen Website. For Matish 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, Matish 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. Because the Government has already provided Matish 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*. *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 discovery requests regarding the Government's chain of custody of the NIT are cumulative and unnecessary.

First, Matish'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 both the Tsyklevich and Miller declarations, Matish 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 Dr. Matthew Miller (hereinafter, “Miller Decl.”) ¶ 3. 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. Decl. of Tsyklevich (hereinafter, “Tsyklevich Decl.”) ¶ 4. In reality, the NIT is one component, which is the computer instructions delivered to Matish’s computer that gathered his identifying information after he logged into the Playpen website. Decl. of Special Agent Daniel Alfin (Ex. 1)(hereinafter, “Alfin Decl.”) ¶ 5. As noted before, those instructions, and the information obtained via their execution, have been made available for review. *Id.*

Particularly, Matish seeks disclosure of the “exploit” in order to determine whether the government “executed additional functions outside the scope of the NIT warrant.” Tsyklevich 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 Matish’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 Matish’s computer is purely theoretical. Alfin Decl. ¶ 14. While it is possible for some 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 Matish’s computer system or security firewall that would warrant concern that the identifiers misidentified Matish as a Playpen user. *Id.* To alleviate Matish’s concerns about the “exploit,” the Government has offered to allow the Defense to review the two-way network data stream

transmitted to the FBI from Matish's computer after the NIT's deployment. Alfin Decl. ¶ 15. Reviewing the data stream would show the Defense that the data sent from Matish's computer is identical to the data the government provided as part of discovery. Alfin Decl. ¶ 16.

Additionally, Matish 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 has agreed to provide a copy of the data stream sent by Matish'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 Matish's computer is in fact what was sent by Matish's computer. *Id.* The Government has confirmed that the information sent to the government from Matish's computer is exactly what the government disclosed in discovery as obtained by the NIT. *Id.*

Lastly, Matish 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. Tsyerklevich 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. Matish'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 “Broden” 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.

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

Matish classifies the NIT as “malware,” and accordingly argues the possibility that the NIT may have opened the door for other entities to download illicit material onto his computer without his knowledge. To obtain the source code and subsequently present to the jury that the child pornography came from some other source, Matish 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. If Matish 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 Matish’s case, the entire source code is not material to his defense because the evidence does not indicate the possibility that Matish unknowingly obtained child pornography.

First, the Defense incorrectly asserts that the NIT is undisputedly malware by claiming

that it compromised and overrode Matish's computer security settings. Def. Reply to Gov. Response to Compel Disc. p. 5. He treats that assertion as fact. In actuality, none of the defendant's expert declarations make so bold a claim. At best, they merely contend that it would be possible for an exploit to do so. That is a significant and material difference.

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 Matish's computer; it merely interacted with his computer to obtain the information that traced him to the "Broden" account. Alfin Decl. ¶ 6. Further, after the NIT sent instructions to Matish'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, Matish points to no facts to suggest otherwise.

Should the defense decide to further inquire about any potential malware that could have been left on Matish's computer, his devices are available for review. Alfin Decl. ¶ 35. However, the defense has declined to review 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. Mr. Matish'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 Matish's computer rather than Matish 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. Matish only speculates as 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.

#### **IV. 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 Matish'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. 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. Stone Aff. of Robert Stone (Ex 2 *under seal*)(hereinafter Stone Aff.) ¶5. The government presents detailed and specific information pertaining to the sensitivity of the programming code in its separate *ex parte, in camera* submission. However, the broad outlines of those concerns are presented herein and in the Stone Affidavit, a copy of which has been provided to Matish.

The privilege has its roots in *United States v. Roviato*, 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 *Roviato* to cover other investigative techniques, including traditional and electronic surveillance. For example, in *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.

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 Roviato*, 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 is explained in more concrete terms in the government’s separate *ex parte, in camera* materials, 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 and his failure to timely seek to compel its disclosure. 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.<sup>3</sup> Accordingly, in the event the Court finds the requested

---

<sup>3</sup> 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.”).



information to be material, the Court should review the government's separate *ex parte*, *in camera* materials 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 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.<sup>4</sup> 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 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 has provided, as it did in

---

<sup>4</sup> An "aircard" may be attached to a laptop in order to provide Internet service.

*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, and forensic images of his computers and devices, 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 the defendant 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 above reasons, the defendant's motion to compel should be denied.

Respectfully submitted,

DANA J. BOENTE  
UNITED STATES ATTORNEY

By: \_\_\_\_\_/s/\_\_\_\_\_  
Eric M. Hurt  
Assistant United States Attorneys  
Virginia State Bar Nos. 35765  
Fountain Plaza Three, Suite 300  
721 Lakefront Commons  
Newport News, VA 23606  
Phone: (757) 591-4000  
Fax: (757)591-0866  
Email: [Eric.hurt@usdoj.gov](mailto:Eric.hurt@usdoj.gov)

\_\_\_\_\_/s/\_\_\_\_\_  
Alanna Trivelli  
Third Year Law Student

\_\_\_\_\_/s/\_\_\_\_\_  
Haley Morton  
Third Year Law Student

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 1<sup>st</sup> 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:

Andrew W. Grindrod  
Assistant Federal Public Defender  
Office of the Federal Public Defender  
150 Bousch Street, Suite 403  
Norfolk, Virginia 23510  
Andrew\_Grindrod@fd.org

Richard J. Colgan  
Assistant Federal Public Defender  
Office of the Federal Public Defender  
150 Bousch Street, Suite 403  
Norfolk, Virginia 23510  
Richard\_Colgan@fd.org

\_\_\_\_\_/s/\_\_\_\_\_  
Eric M. Hurt  
Virginia State Bar No. 35765  
Assistant United States Attorney  
Attorneys for the United States  
United States Attorney's Office  
Fountain Plaza Three, Suite 300  
721 Lakefront Commons  
Newport, VA 23606  
Phone: 757-591-4000  
Email: eric.hurt@usdoj.gov

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
NEWPORT NEWS DIVISION

UNITED STATES OF AMERICA )  
 )  
v. ) CRIMINAL NO. 4:16cr16  
 )  
EDWARD JOSEPH MATISH, III )

DECLARATION OF SPECIAL AGENT DANIEL ALFIN

Your affiant, Daniel Alfin, being duly sworn and deposed, states the following:

1. I am a Special Agent of the Federal Bureau of Investigation. I am currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit. My duties involve the investigation of individuals using various types of technology to produce, distribute, and trade child pornography. As an Agent assigned to the FBI Violent Crimes Against Children Section, Major Case Coordination Unit, I routinely analyze network data that has been collected pursuant to court order. I hold a University Degree in Information Technology and multiple industry certifications that are recognized by the United States Department of Defense. Additionally, I have completed all stages of FBI Cyber Training including courses on Advanced Network Investigative Techniques, Network Traffic Analysis, Ethical Hacking, and Malware Analysis.

2. Analysis of network data generally consists of identifying the origin, destination, and content of communications that are sent across the Internet. In addition to performing this type of analysis, I am routinely called upon to assist Agents across the FBI with similar analysis. In the past two years, I have analyzed data from more than 30 court-authorized network intercepts and those analyses have been used in affidavits and court filings in several judicial districts.

3. I have been involved in the FBI investigation of the Playpen website since it came online in approximately August 2014. Playpen was a website that existed on an anonymous network and was dedicated to the advertisement and distribution of child pornography. My duties included the review of Playpen's content on multiple occasions, engagement in undercover activities on Playpen, and the coordination of investigative activity aimed at identifying members of Playpen, including the defendant, Edward Matish.

4. In preparing this declaration, I have reviewed evidence and spoken with FBI personnel familiar with the facts and circumstances outlined below. I provide the following summary of the information I have learned as a result.

5. I have also reviewed the declaration of Messrs. Tsyklevich and Miller, the defense experts, respectively dated January 13, 2016 and May 23, 2016, (hereinafter “Tsyklevich Dec.” and “Miller Dec.”) and noted a number of statements that are inaccurate and/or require clarification. I will address several of these in great detail below but will begin by noting one overarching misconception in these declarations. Specifically, Tsyklevich and Miller attempt to redefine the NIT as something containing multiple components. The NIT, however, consists of a single component: that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI. Those computer instructions, and the information obtained via their execution, have been made available for review in this case. In his expert declarations, Matish describes that component as a “payload.”

6. As another threshold matter, I would note that I do not consider the NIT used by the FBI to be “malware,” though the experts retained by Mr. Matish describe the NIT in such terms. The word malware is an amalgamation of the words “malicious” and “software”. The NIT utilized in this investigation was court-authorized and made no changes to the security settings of the target computers to which it was deployed. As such, I do not believe it is appropriate to describe its operation as “malicious.”

7. The NIT computer instructions provided to the defense on May 26, 2016 comprise the only “payload” executed on Matish’s computer as part of the FBI investigation resulting in his arrest and indictment in this case. Accordingly, the defense has been given access to the only “payload” as that term is used by the defense in the Tsyklevich declaration.

8. After the NIT collected the information that it was permitted to collect via the computer instructions sent to Matish's computer, there was nothing that resided on Matish’s computer that would allow the government (or some other user) to go back and further access that computer.

9. I have personally executed the NIT on a computer under my control and observed that it did not disable the security firewall, make any changes to the security settings on my computer or otherwise render it more vulnerable to intrusion than it already was. Additionally, it did not “infect” my computer or leave any residual malware on my computer.

10. Matish claims via his expert declarations that the NIT consisted of four components – an “exploit,” a “payload,” software that generates a payload and injects a unique identifier into it, and a server component that stores the delivered information. Tsyklevich Dec. p. 2 ¶ 4.

11. As used here, a computer “exploit” consists of lines of code that are able to take advantage of a software vulnerability. In layman's terms, an “exploit” could be thought of as a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key. Here, an “exploit” allowed the FBI to deliver a set of instructions-the NIT-to Matish's computer. Those instructions then gathered specified information, including Matish's IP address, and transmitted that information to government controlled computers. The NIT instructions and results have been provided to the defense for review; the “exploit” has not.

12. Tsyklevich claims that he requires access to the government's “exploit” to determine if the government “executed additional functions outside the scope of the NIT warrant.” Tsyklevich Dec. p. 3, ¶ 6. He is wrong. Discovery of the "exploit" would do nothing to help him determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Matish's computer, not what it did once deployed.

13. The Miller declaration states that “[a] computer system that has been exploited has been fundamentally altered in some way.” Miller Dec. p. 2, ¶ 5. Miller cites no authority for that premise. It is incorrect. It is possible for an existing vulnerability in a computer system to be exploited without making any fundamental changes or alterations to that computer system. The Miller declaration also speculates about consequences that may occur “if the security firewall on a computer is disabled by an NIT or other malware.” Miller Dec. p. 3, ¶ 7.

14. It is theoretically possible for an exploit to make fundamental changes or alterations to a computer system or to disable its security firewall. However, as noted above, the NIT used here and the exploit used to deliver it did not do so. Other than to point to this theoretical possibility, I am aware of no evidence or indication to which either defense expert points to suggest otherwise.

15. The government has advised the defense that it is willing to make available for its review the two-way network data stream showing the data sent back-and-forth between Matish's computer and the government-controlled computer as a result of the execution of the NIT.

16. Review of this data stream reflecting the information transmitted to the FBI from Matish's computer as a result of the deployment of the NIT confirms that the data sent from Matish's computer is identical to the data the government provided as part of discovery.

17. Review of the network data stream also confirms that that no images were transmitted from Matish's computer to a government-controlled computer or from a government-controlled computer to Matish's computer as a result of the execution of the NIT.



18. Discovery concerning the “server component” is unnecessary because there are alternative means of verifying the accuracy of the NIT information.

19. Tsyklevich claims that he needs access to the server component in order to confirm that the information obtained from Matish's computer by the NIT and sent to the FBI was accurately stored and reproduced. Tsyklevich Declaration pp. 3-4. The defense does not need access to government servers to do this, however, because the government has agreed to provide an alternative method of verifying that the information obtained from Matish's computer was accurately recorded. Specifically, the government has offered to provide a copy of the data stream sent by Matish's computer to the government as a result of the execution of the NIT. Tsyklevich can compare the information sent to the government by the NIT to the information provided in discovery to verify that what the government recorded from Matish's computer is in fact what was sent by Matish's computer. I have reviewed that data stream and, as explained below, confirmed that the information sent by Matish's computer as a result of the NIT matches the information that is stored on the government's servers.

20. When two computers communicate via the Internet, they do so using standard network protocols. Communications over the Internet are sent in “packets,” which serve as the means by which computers share information over a network. Just as two people communicating over email exchange individual messages, computers exchange network packets. These packet exchanges follow standard network protocols that permit individual computers to process and exchange information with one another. Just like two people meeting on the street, computers wishing to communicate with one another first exchange greetings through a “handshake,”<sup>1</sup> then exchange information, and part ways with a communication exchange that basically consists of the computers saying “goodbye” to each other.

21. Here, when the NIT was delivered to Matish's computer, it had exactly this sort of interaction with a government-controlled computer. The network packets memorializing this exchange, which have been preserved in a standard file format, make it possible to reconstruct that exchange and see exactly what information was transmitted by Matish's computer to the government.

22. A review of the data file, known as a PCAP file, documenting the exchange contains several network packets exchanged between Matish's computer and the government computer. The initial packets correspond to the initial “handshake” that established the connection between Matish's computer and the government computer. Similarly, the final packets in the

---

<sup>1</sup> Some protocols that are used to communicate via the Internet do not include a “handshake” as described in this declaration. These other protocols are not relevant to the matter at hand as the communications that occurred as a result of the deployment of the NIT did utilize a network protocol that included a “handshake”.

communication correspond to the "goodbye" communication between the two computers. The remaining packet(s) thus contains the substance of the communication, namely, the information collected by the NIT after it was delivered to Matish's computer.

23. Reviewing these packets, I was able to confirm that the information collected from Matish's computer matches the information stored on the government servers that has been provided in discovery. Each of the pieces of information the government-controlled computer recorded being collected from Matish's computer by the NIT appears in the packets. If Tsyркlevich's goal is to verify the accuracy of the information stored by the government, then a review of the network data is all that would be required. The data is not encrypted or redacted thus making such a review possible.

24. Tsyркlevich maintains that he needs access to the computer code that "generates a payload and injects a unique identifier" in order to ensure the identifier used was in fact unique. Tsyркlevich Dec. p. 3 ¶ 6. He is wrong because the unique identifier assigned to Matish's NIT results was in fact unique.

25. Prior to deployment of the NIT, a unique identifier is generated and incorporated into the NIT. When the "activating computer" sends information to the government as a function of the NIT, that unique identifier is included with the response. When the information is received by the government, a check is performed to ensure that the unique identifier contained within the delivered information matches the unique identifier that was generated by the government. In the matter at hand, all identifiers received by the government, including the one sent by Matish's computer, did match identifiers that were generated by the government and they were in fact unique.

26. The ultimate question posed by Tsyркlevich is not how the unique identifier was generated but if the unique identifier sent to Matish's computer was actually unique. I have reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated.

27. A query of an FBI database containing the information gathered as part of this investigation through the use of the NIT revealed the following: 1) there are no duplicate unique identifiers within the database, meaning that each identifier assigned to an individual Playpen user is in fact unique; 2) the identifier associated with the username "Broden" was in fact unique; and 3) there are no identifiers in the database other than those generated by the deployment of a NIT as part of this investigation; the significance of which is the fact that this proves no outside entity tampered with or fabricated any of the unique identifiers generated as part of the investigation.

28. I have read the Defendant's reply to the Government's Response to the Motion to Compel dated May 23, 2016. In the motion, Matish asserts that there are chain of custody problems caused by the fact that the NIT transmitted data "unencrypted over the traditional internet". This assertion is further supported by the declaration of Matthew Miller who states "the IP address relayed to the FBI was unencrypted and subject to attack by hackers" Miller Dec. p. 3 ¶ 9. He is wrong. In fact, the network data stream that has been made available for defense review would be of no evidentiary value had it been transmitted in an encrypted format. Because the data is not encrypted, Matish can analyze the data stream and confirm that the data collected by the government is within the scope of the search warrant that authorized the use of the NIT. Had the data been transmitted in an encrypted format the data stream would be of no evidentiary value as it could not be analyzed. Additionally, Miller demonstrates a lack of understanding of how data is transmitted over the internet. Computers that communicate over the internet do so by use of IP Addresses. While the data that is sent and received by the computers may be encrypted, the IP Addresses cannot be encrypted as Miller suggests they should be.

29. Also contained within the defendant's Motion to Compel Discovery is the statement, "defense needs the NIT code to verify the government's allegations that it deployed the NIT based on some specific action taken by Mr. Matish." Motion. p. 2 ¶ 2. This statement is wrong and is not supported by any expert declaration filed on behalf of Mr. Matish. In fact, the Playpen user report for the user "Broden" contains a detailed breakdown of all actions taken by the user "Broden" on the Playpen website including the exact action that triggered the NIT; the accessing of a specific post on the Playpen website that depicted what appeared to be several images of a prepubescent female whose genitals were being licked by a dog.

30. In each instance when I have been tasked with identifying and analyzing malware<sup>2</sup>, I did not have advance knowledge of the specific malware for which I was looking or even if malware was actually present, though there was reason to suspect the presence of malware. I have nonetheless been able to locate, identify, and analyze suspected malware notwithstanding the lack of advance knowledge about the particular malware. In this declaration, I will lay out in general terms some of the steps that can be taken to identify and analyze malware and provide additional detail concerning the operation of the NIT used in the FBI investigation at issue in United States v. Matish.

31. Prior to analyzing a device for traces of a malware infection and even without knowledge of the specific type of malware involved, an investigator generally has some information or indication of the presence of malware. For example, an individual's computer could be

---

<sup>2</sup> The term "malware" generally refers to computer software that impairs the integrity or availability of data, a program, a system, or information. Other common terms that describe various types of malware are "virus", "trojan", and "worm".

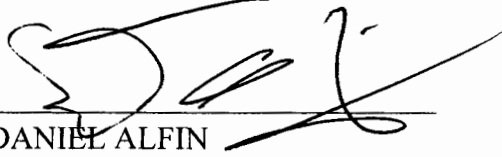
experiencing problems with programs failing to operate as intended or a user may notice that data have inexplicably been deleted from the system.

32. If malware does in fact transmit data over the Internet in a similar fashion to how the NIT transmitted data to an FBI controlled computer server, having a copy of the transmitted network data would be a valuable tool that would assist with analyzing a system and searching for malware. If the network data is not encrypted, it will generally contain strings of plain text containing identifiers that can be used as search terms during the course of a forensic analysis. Although the defense has declined to review the network data available in this case, I have reviewed and analyzed that network data. My review confirmed that it is not encrypted and contains various strings that would generally be considered valuable during the course of forensic analysis. For example, a defense expert who suspects that a given device was a target of the NIT could use these search terms to try and assess whether there are any traces of the NIT still left on the target device or if the NIT otherwise remains on the device.

33. Utilization of search terms is just one avenue of analysis available to locate and identify malware on a device. It is also possible to review the list of programs designated to run when a device's operating system loads. Such a review is a crucial step in determining whether a computer may be infected with malware. After identifying and eliminating from consideration known programs that the user intended to execute upon startup, an investigator may focus on any remaining programs whose purpose is unknown. In some instances, malware can be disguised as a legitimate program and can be identified by comparison of the legitimate program's file hash value against the hash value of the suspect program.

34. Where there is reason to suspect a storage device such as a USB drive or even a cellular telephone has been infected with malware, an investigator can undertake a dynamic analysis of any suspect files on that device and verify that those files either do or do not have the ability to execute malicious code. The process of conducting a dynamic malware analysis generally involves creating a copy of a suspect file and executing it in a test environment. The state of the test environment is recorded prior to execution of the file and various programs are active in the test environment that record changes to the system. Additionally, various pieces of software or hardware can be utilized to capture any network data generated by the file upon execution.

35. The devices seized from Mr. Matish are available to the defense for inspection and review, and I believe, based on my training and experience, that the procedures describe above (among others) could be applied to those devices to determine whether there is evidence suggesting that the NIT or a piece of malware was responsible for the collection of child pornography found on Mr. Matish's devices.



---

DANIEL ALFIN  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION

Affidavit of  
Robert Stone  
Special Agent  
Federal Bureau of Investigation  
(Filed under seal)