UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

UNITED STATES OF AMERICA

vs. Case No. 2:16-cr-134-FtM-29MRM

DAVID CASWELL,

Defendant.
_____/

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The Defendant, DAVID CASWELL, by and through the undersigned attorney, moves this Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) to suppress the following: (1) all evidence, including electronic information, obtained from the Government's illegal search of Mr. Caswell's computer through the use of Government malware, in violation the Fourth Amendment, 28 U.S.C. §636(a), and Fed. R. Crim. P. 41; (2) all evidence obtained from the Government's illegal search of Mr. Caswell's residence, based upon a tainted local search warrant; and (3) all statements obtained from the Government's custodial interrogation of Mr. Caswell, in violation of *Miranda v. Arizona*, 384 U.S. 436 (1966). In support of the motion, Mr. Caswell states as follows:

FACTS

1. The Defendant is charged with Count 1- Possession of Child Pornography, 18 U.S.C. §2252(a)(4)(B) and (b)(2).

2. The events leading to the charged offenses stemmed from a Government investigation, in February 2015, into a website known as "Playpen".[1] (*See generally* the instant case's "Affidavit in Support of Search Warrant", No. 2:15-mj-1096-MRM (M.D. Fla. July 27, 2015)(hereafter "Naples Affidavit"); *see also generally* "Affidavit in support of Application for Search Warrant", No. 1:15-SW-89 (E.D. Va. Feb 20, 2015)(hereafter "NIT Affidavit").
3. The Government has described Playpen as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children online." (Naples Affidavit, at 13 ¶11).
4. Government investigators seized Playpen computer server in North Carolina and brought it to a Government facility in Virginia. (*Id.*)
5. The FBI assumed administrative control over the website and continued to operate the Playpen website in Virginia. (*Id.*)
6. The Playpen website operated on an anonymous network known as "The Onion Router" or "TOR" network. (NIT Affidavit, at 10 ¶7).
7. The TOR network prevents law enforcement from obtaining the Internet Protocol addresses (I.P. addresses) of the users. (*Id.* at 11 ¶8).
8. Specifically, TOR software protects user privacy by bouncing user computer communications through a network of worldwide computers. When a user accesses a

[1] The website was referenced as "Target Website" in the NIT Affidavit, and "Website A" in the Naples Affidavit; but the website has since been deactivated and widely reported as "Playpen." *See, e.g., United States v. Adams, slip*, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016).

website, through the TOR network, the IP address of the last computer through which the user's communications were routed is displayed (the "exit node"), not the I.P. address of the user's actual computer. (*Id.*)

9. On or about February 20, 2015, the Government sought, and obtained, a search warrant authorizing the deployment of a Network Investigative Technique (hereafter "NIT"), which was issued by a federal magistrate judge in the Eastern District of Virginia. A NIT is computer code- like a virus or malware- the Government sends to a suspect computer. (*See* NIT Affidavit; *see also* "Search and Seizure Warrant", No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015)(hereafter "NIT Warrant")).
10. The NIT Affidavit was prepared by a veteran FBI agent, who was assigned to a unit tasked with specifically investigating child pornography.
11. The NIT Warrant application indicated that the place to be searched was the Playpen server now in Virginia. (NIT Affidavit, at 32).
12. However, the NIT Warrant application also noted that individual users cannot be identified by examination of the Playpen server, due to the use of the TOR network. (*Id.* at 11-12).
13. Generally, a user's computer would download a website's content, in order to display web pages on a user's computer. In the case of the TOR network, the content would be relayed through multiple computers and back to the user's computer. The NIT supplemented the Playpen content, and sent instructions to the user's computer. (*Id.* at 11 ¶8, *and* 24 ¶33).

14. The NIT instructions caused the user's computer to then send data to a separate Government computer, specifically the actual I.P. address, the date/time of Playpen use, the type of computer operating system, and other identifying information of the user. (*Id.* at 24-26).

15. The Government allowed the Playpen website to remain in use from February 20, 2015 to March 4, 2015. (Naples Affidavit, at 13 ¶11).

16. The Government states that during the time it operated the Playpen website, the FBI deployed a NIT to a computer believed to be connected with Playpen user "whaddupyall" and extracted the I.P. address along with other identifying information. (*Id.* at 20).

17. FBI investigators used this information to issue an administrative subpoena to Comcast for information related to the I.P. address, and in doing so identified David Caswell as the internet subscriber for the identified I.P. address, and determined Mr. Caswell's physical address of 3090 42nd Street SW, Naples, Florida 34116. (*Id.* at 21-22).

18. Special Agent Zachary Ewert, a member of the Child Exploitation Task Force and detective with the Collier County Sheriff's Office, submitted a search warrant application for the Defendant's physical address. (*See generally* Naples Affidavit).

19. Specifically, Agent Ewert alleged that user "whaddupyall" was logged into the Playpen website for a total of fifteen (15) hours from the dates of January 26, 2015 to March 4, 2015. The Playpen showed that this user accessed three posts that contained links to child pornography. The warrant application did not allege that the images

were viewed or downloaded. (*Id.* at 20-21). The warrant application also did not allege that Mr. Caswell uploaded or downloaded images. (*Id.*)

20. The search warrant was issued by Magistrate Judge Mac R. McCoy of the Fort Myers Division of the Middle District on July 27, 2015, and executed on August 6, 2015. ("Search and Seizure Warrant", No. 2:15-mj-1096-MRM (M.D. Fla. July 27, 2015)(hereafter "Naples Warrant")).

21. Government agents seized various computer and electronic devices during the search of the Defendant's residence.

22. When executing the search warrant at the Defendant's residence, Government agents began questioning Mr. Caswell. Agents told the Defendant that he was free to leave, but his children were sleeping inside the residence. During the interview, the Defendant repeatedly asked to call his wife, but agents ignored his requests. The Defendant was not read a *Miranda* warning prior to this questioning.

23. After repeated questioning, the Defendant allegedly stated that he had accessed the Playpen website, and admitted having images on his personal computer.

ARGUMENT

The Court should suppress the physical evidence and the Defendant's statements to law enforcement.

I. THE PHYSICAL EVIDENCE SHOULD BE SUPPRESSED DUE TO AN ILLEGAL SEARCH OF THE DEFENDANT'S COMPUTER.

The Defense requests that the Court suppress the physical evidence seized from the Defendant because: (1) the Defendant had a reasonable expectation of privacy in his personal

computer located in his residence; (2) the search of the Defendant's computer violated the Fourth Amendment of the United States Constitution; (3) the search of the Defendant's computer was also in violation of Rule 41 of the Federal Rules of Criminal Procedure; (4) the illegal search of the Defendant's computer tainted Naples Warrant; and (5) suppression is the appropriate remedy.

1. The Defendant had a reasonable expectation of privacy in his computer.

The focus of this Court's analysis should be on the Defendant's computer, because this is where the Government illegally extracted electronic data. While a defendant generally does not have an expectation of privacy in an I.P. address, *United States v. Adams*, No. 6:16-cr-11-Orl-40GJK, slip op., 2016 WL 4212079, at 3-4 (M.D. Fla. Aug. 10, 2016), Mr. Caswell's I.P. address was only discovered by searching his computer with the illegal NIT. It is important to recognize that distinction. In *United States v. Adams*, an identical case involving the Playpen website and the same NIT Warrant at issue, a Middle District of Florida judge reasoned:

> There is little doubt that had law enforcement officers obtained Defendant's I.P. address from a non-Tor-based server and issued a subpoena to the [internet service provider] to determine Defendant's physical address, a motion to suppress the information obtained from the [internet service provider] would be without merit. However, Defendant's I.P. address was discovered only after property residing within the Defendant's home- his computer- was searched by the NIT.
> *Id.* at 4.

In the instant case, law enforcement noted that it could not have determined the Defendant's I.P. address had the NIT not been deployed on the Defendant's computer. The

NIT then caused the Defendant's computer to transmit information, including the I.P. address. The search occurred on the Defendant's computer, in his residence, in Florida. As in *Adams*, the Defendant held a reasonable expectation of privacy in his home computer. *Id.*

2. The Defendant's computer was searched in violation of the Fourth Amendment.

At its core, this motion is about the Government's illegal search of the Defendant's computer in violation of the Fourth Amendment. Federal agents exceeded the plain language of the NIT Warrant designating the particular place to be searched. As the Court is well aware, the Fourth Amendment of the United States Constitution protects citizens from unreasonable Government searches. Specifically, the Fourth Amendment provides the protection that, "...no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched...." U.S. Const. amend. IV.

The NIT Warrant states that the property to be searched is located in the Eastern District of Virginia, and specifically identified in "Attachment A" of the NIT Warrant Application. "Attachment A" describes the "place to be searched" as:

> **ATTACHMENT A**
>
> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL- upf45jv3bziuctml.onion – which will be located at a government facility in the Eastern District of Virginia.

> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

The above language is clear; the Eastern District of Virginia magistrate approved an Eastern District of Virginia search- a search of the Playpen website server. The warrant did not authorize a search in another location, and the NIT did not search in the Eastern District of Virginia. In reality, the NIT software piggybacked on the Playpen website web content to the user's computer, wherever it was located. As the Playpen website content uploaded on the user's computer, so did the NIT, much like a computer virus or malware. The user's computer was then infected with instructions commanding the computer to transmit data to a separate Government computer in Virginia. In the instant case, the actual NIT search occurred, not on the Playpen server, but rather on Mr. Caswell's computer.

Such a concept of following the warrant language is so elementary, that is sometimes forgotten. The agents exceeded the scope of the NIT Warrant. Consequently, the search in Florida was outside the scope and in violation of the Fourth Amendment.

3. The Defendant's computer was searched in violation of Rule 41(b).

Assuming the Virginia magistrate understood the method of the NIT search, the NIT Warrant still violated federal law. The United States Code gives "[e]ach United States magistrate judge...all powers and duties conferred...by law or by the Rules of Criminal Procedure...." 28 U.S.C. 636(a)(1). Rule 41 of the Federal Rules sets geographic limitations to a magistrate's powers; one such geographic limitation limits the issuance of warrants. A

search warrant which exceeds the geographic boundary of a magistrate's power is not a mere technicality. Such a warrant would be void *ab initio*, and any search stemming from the void warrant would be without legal authority. Consequently, suppression is warranted in such a scenario. *See, e.g., United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015). In the case at bar, the NIT Warrant was void ab initio, because the issuance of the warrant violated the jurisdictional limitations placed upon the Eastern District of Virginia magistrate.

A. Rule 41

At the time of the NIT Warrant issuance, Rule 41(b) provided a magistrate judge with authority to issue a search warrant in five circumstances, which were enumerated in five Rule 41(b) subsections[2]. Fed. R. Crim. P. 41(b)(2015 version). Two of these subsections can be dismissed outright, based upon the plain language, as providing a basis of legal support for the NIT Warrant issuance. Rule 41(b)(3) is inapplicable as Mr. Caswell's case does not involve "domestic or international terrorism." Similarly, Rule 41(b)(5) can also be dismissed as a basis of support for the NIT Warrant because Mr. Caswell's computer was not located within any of the specified locations of that subsection. While the remaining subsections (Rule 41(b)(1), 41(b)(2), and 41(b)(4)) require more discussion, analysis of these subsections still shows that the NIT Warrant was void *ab initio*.

[2] As Rule 41(b) was revised in 2016, and for ease of seeing the complete text of Rule 41(b) in existence in 2015, *see, e.g., United States v. Levin*, 186 F. Supp.3d 26, 32-33 (D. Mass. May 5, 2016).

B. Rule 41(b)(1) does not apply as the "search" occurred in Florida.

Rule 41(b)(1) does not validate the issuance of the NIT Warrant. Similar to the preceding Fourth Amendment discussion, this subsection offers no support, because the NIT searched in Florida. Rule 41(b)(1) states:

> **(b) Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district...has authority to issue a warrant to ***search*** for and seize...**property located within the district**.... Fed. R. Crim. P. 41(b)(2015 version)(emphasis added).

Rule 41(b)(1) allows a magistrate to issue a search warrant for property located within that magistrate's own district. In this case, this subsection would provide support if the search and searched property was located in the Eastern District of Virginia. It wasn't. The NIT Warrant inaccurately states that the property to be searched is "located in the Eastern District of Virginia." Attachment A to the NIT Warrant indicates that the computer server, located in Eastern District of Virginia, is the place to be searched. Yet, the actual "place to be searched" was any computer that would unknowingly download the NIT, thereby forcing the transmission of their internal computer data back to the FBI in Virginia. The NIT Warrant authorized these searches even though there was no basis from which to conclude that these computers would be located in the Eastern District of Virginia. And in Mr. Caswell's case, the searched computer was in Florida. Rule 41(b)(1) cannot justify the search of the Defendant's computer.

Removing any doubt whether it was the Defendant's computer that was searched rather than the Virginia server, the Government explained the need for the NIT on the basis that possession of the Playpen server alone would not allow the Government to identify the site's users. (NIT Affidavit, at 11-12). In order to do so, it was necessary to deploy the NIT so that a user's computer would download the NIT and allow the Government to seize the identifying information before sending it back to Virginia. Although the NIT was first deployed from the server in Virginia, it is clear that the actual search occurred when the NIT was installed on the defendant's computer and extracted its data. This situation is no different from agents claiming that a search took place in Virginia because they traveled to Florida, copied data from a computer, and returned to Virginia before examining the contents.

In a similar case to instant one, a federal court judge rejected the argument that the NIT search occurred in the Eastern District of Virginia- the location of the Playpen server. *United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at 6 (W.D. Wash. Jan. 28, 2016). The *Michaud* opinion reasoned, "...because the object of the search and seizure was [the defendant's] computer, not located in the Eastern District of Virginia, this argument fails." *Id.*

A similar conclusion was reached in the in the denial of a search warrant application. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp.2d 753 (S.D. Tex. Apr. 22, 2013)("*In re Warrant*"). There, as the location of the target computer was unknown, the Government argued authority stemmed from Rule 41(b)(1) by reasoning that the "information obtained from the Target Computer will first be examined in this judicial

district." *Id.* at 756. In rejecting the warrant application, the *In re Warrant* opinion explained that the search of data occurs "...not in the airy nothing of cyberspace, but in physical space with a local habitation and a name." *Id.* at 757. The same is true here. The NIT search did not occur in Virginia or in cyberspace. It was a physical search of the Defendant's computer which was located in Naples, Florida.

A Middle District of Florida judge has also rejected the argument that the NIT search, at issue, occurred in the Eastern District of Virginia. *Adams*, 2016 WL 4212079, at 5. The *Adams* opinion noted that such an argument "...misses the point that Rule 41(b) address[ed] the location of the property to be searched...." and found that the search occurred on the defendant's computer outside the Eastern District of Virginia. *Id.* While the case is not controlling, the analysis is certainly persuasive as the facts are directly on point. Mr. Caswell asks the Court to adopt the reasoning that Rule 41(b)(1) does not apply.

C. Rule 41(b)(2) does not apply as the computer was never in Virginia.

Similar to the preceding analysis, Rule 41(b)(2) also inapplicable because Mr. Caswell's computer was not in the Eastern District of Virginia at the time of the NIT Warrant issuance. Rule 41(b)(2) states:

> **(b) Authority to Issue a Warrant.** At the request of a federal law enforcement
> officer or an attorney for the government:
>
> > (2) a magistrate judge with authority in the district has authority to issue a warrant for...property outside the district if the...***property is located within the district when the warrant is issued but might move***

> ***or be moved outside the district before the warrant is executed***;
>
> Fed. R. Crim. P. 41(b)(2015 version)(emphasis added).

This subsection allows an extraterritorial search of property, if the property is located within the district when the warrant is issued, but might later move or be moved before the warrant is executed. This subsection fails to provide support because the Defendant's computer was never physically within the Eastern District of Virginia. *See Michaud*, 2016 WL 337263 at 6 (finding "unconvincing" the argument that Rule 41(b)(2) applies). Importantly, the court in *In re Warrant* noted:

> That (b)(2) does not authorize a warrant in the converse situation- that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment's reflection reveals why this is so, If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might be initially found.
> *In re Warrant*, 958 F. Supp. 2d at 757.

This subsection offers no justification for the search of the Defendant's computer.

D. Rule 41(b)(4) does not apply as the NIT was not a "tracking device".

As the NIT "software would be installed on a computer whose location could be anywhere on the planet," *In re Warrant*, 958 F.Supp.2d at 758(rejecting Rule 41(b)(4) as support for search warrant for computer), and as the NIT searches the user's computer, this subsection is also inapplicable. Rule 41(b)(4) states:

> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a

> tracking device; the warrant may authorize use of a device to *track the movement of...property located within the district, outside the district, or both; and*
>
> Fed. R. Crim. P. 41(b)(2015 version)(emphasis added).

Rule 41(b)(4) allows for tracking devices to be installed within the issuing district on property that may travel to outside the district. The NIT was installed on the defendant's computer in Florida, which was never physically located within the Eastern District of Virginia. *See Michaud*, 2016 WL 337263 at 6. Even if the installation were deemed to have occurred on the server in Virginia, section (b)(4) is inapplicable because the Defendant "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." *Id.*

The *Adams* opinion offered a detailed analysis for its rejection of the argument that the NIT Warrant was a tracking device:

> The Government offers a tempting interpretation of [Rule 41(b)(4)] by comparing the placement of the NIT onto the government-controlled Playpen server to the concealment of a tracking device in a container holding contraband which is then tracked outside of the district where the warrant was issued. However, by the Government's admission, once installed on the Playpen server, the NIT does nothing until the user logs onto the government-controlled server in that district and downloads the NIT. ***The warrant authorizes the installation of the NIT onto the government-controlled Playpen server and not onto Defendant's computer, which is located outside of the Eastern District of Virginia. Moreover, the NIT does not track; it searches.*** As discussed above, the NIT is designed to search the user's computer for certain information, including the IP address, and to transmit that data back to a server controlled by law enforcement.
> *Adams*, 2016 WL 4212079, at 6 (emphasis added).

Mr. Caswell acknowledges that some federal district courts have found the NIT Warrant to be a "tracking device", but asks this Court to adopt the sounder logic of the federal courts that have rejected this argument. *Adams*, 2016 WL 4212079, at 6; *Michaud*, 2016 WL 337263, at 6. *See also United States v. Levin*, 186 F. Supp.3d 26, 34 (D. Mass. May 5, 2016); *United States v. Croghan*, ---F.Supp.3d---, 2016 WL 4992105, at 4-5 (S.D. Iowa Sept. 19, 2016); *United States v. Henderson*, 2016 WL 4549108, at 3-4 (N.D. Cal. Sept. 1, 2016); *United States v. Werdene,* 188 F.Supp.3d 431 (E.D. Pa. May 18, 2016); *United States v. Workman*, ---F.Supp.3d---, 2016 WL 5791209, at 4 (D. Colo. Sept. 6, 2016); *United States v. Vortman*, No. 16-cr-00210-TEH-1, 2016 WL 7324987, at 10 (N.D. Cal. Dec. 16, 2016); *United States v. Broy*, ---F.Supp.3d---, 2016 WL 5172853, at 8 (C.D. Ill. Sept. 21, 2016); and *United States v. Ammons*, ---F.Supp.3d---, 2016 WL 4926438, at 6 (W.D. Ky. 2016).

4. Suppression is the appropriate remedy.

Suppression is the appropriate remedy because: (1) the Rule 41 violation was a substantive violation; (2) even if the Court were to find a "technical" violation, suppression is still warranted under Rule 41; (3) the Naples Warrant is invalid due to the taint of the illegal NIT Warrant; and (4) the "good faith" exception does not apply.

A. <u>The Rule 41 violation was a substantive violation.</u>

The NIT warrant was a substantive, constitutional violation and requires suppression. The Fourth Amendment of the United States Constitution mandates:

> The right of the people to be secure in their houses, papers, and effects, against unreasonable searches and seizures, shall not be

> violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.
> U.S. Const. amend. IV.

It is assumed that a magistrate issuing a warrant has the legal authority to do so. And in a scenario where the warrant is issued outside jurisdiction, the warrant is regarded as being void at the outset (void *ab initio*). This is the equivalent of a warrantless search with no exigency.

But to fully understand the violation, one must first distinguish Rule 41 technical violations.

In analyzing the exact NIT Warrant at issue, the *Levin* opinion explained:

> A violation of Rule 41 that is purely technical or ministerial gives rise to suppression only where the defendant demonstrates that he suffered prejudice as a result of the violation....The government apparently submits that all Rule 41 violations "are essentially ministerial," and accordingly that suppression is an inappropriate remedy absent a showing of prejudice...Rule 41, however, has both procedural and substantive provisions—and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and as a result have determined suppression to be unwarranted. By contrast, this case involves a violation of Rule 41(b), which is "a substantive provision."....Thus, it does not follow from cases involving violations of Rule 41's procedural provisions that the Rule 41(b) violation at issue here—which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant---was simply ministerial. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013)(concluding that a Rule 41(b) violation constitutes a "jurisdictional flaw" that cannot be excused as a technical defect").
> *Levin*, 186 F.Supp.3d at 4.

Because the Eastern District of Virginia magistrate lacked the authority to issue the NIT Warrant at all, a void warrant existed and the search of Mr. Caswell's computer

occurred in violation of the Fourth Amendment. The information obtained, and derivative evidence seized, should be suppressed.

B. A Rule 41 technical violation would also warrant suppression.

Should this Court find the NIT Warrant to have been a technical Rule 41 violation, versus substantive, suppression is still warranted. A Rule 41 technical violation, "...requires suppression of evidence only where: (1) there was prejudice in the sense that the search would not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983).

Krueger is an instructive case for this Court to look to in assessing whether prejudice occurred and whether suppression is the appropriate remedy for a Rule 41 violation. 809 F.3d 1109 (10th Cir. 2015). The *Krueger* facts establish that federal investigators learned that child pornography was being distributed over the internet from an I.P. address registered to Krueger. *Id.* at 1111-1112. The agents then obtained a search warrant from a Kansas magistrate, to search Krueger's Kansas residence. *Id.* However, when the warrant was executed, the federal agents learned Krueger was in Oklahoma and took his computer with him. *Id.* Federal agents then obtained a second warrant from a Kansas magistrate, authorizing a search in Oklahoma, which was later executed. *Id.* A federal district court, thereafter, granted the Krueger's motion to suppress, as the Kansas magistrate lacked authority to issue a warrant, under Rule 41, for an Oklahoma search. *Id.* at 1112-1113. In affirming, the *Krueger* court held that the proper standard in assessing Rule 41 prejudice is to

"[a]sk whether the issuing federal magistrate judge could have followed [Rule 41]. Applying this standard, we conclude that Krueger established prejudice in the sense that the Oklahoma search might not have occurred because the Government would not have obtained [the second warrant] had [Rule 41(b)] been followed." *Id.* at 1116.

Mr. Caswell's case is analogous to the facts in *Krueger*. Assuming the federal magistrate intended the NIT Warrant as executed, the search of Mr. Caswell's computer would not have occurred had the federal magistrate, in the Eastern District of Virginia, followed Rule 41(b). At the time of the then existing Rule 41(b), the Virginia magistrate could not have complied with the rule and have issued the NIT warrant for a search in Florida. Consequently, Mr. Caswell has suffered prejudice, as the search would not have otherwise occurred. The information obtained from the computer search, and subsequently obtained evidence, should be suppressed.

C. <u>The Naples search warrant is tainted as "fruit of the poisonous tree".</u>

The Naples Warrant was tainted by the illegal search of Mr. Caswell's computer through the NIT. The exclusionary rule extends to evidence obtained through the exploitation of an earlier unlawful invasion or "fruit of the poisonous tree." *Segura v. United States,* 468 U.S. 796, 804. (1984). Evidence will not be excluded, however, if the connection between the illegal police conduct and the discovery and seizure of the evidence is "so attenuated as to dissipate the taint." *Segura,* 468 U.S. at 805. When a search warrant relies on unconstitutionally obtained information, the warrant is not automatically invalid. Where probable cause exists without the unconstitutionally obtained information, the court does not have to suppress the evidence obtained from the tainted warrant. *United States v. Sims*, 428

F.3d 945, 954 (10th Cir. 2005). "An affidavit containing erroneous or unconstitutionally obtained information invalidates a warrant if that information was critical to establishing probable cause. If, however, the affidavit contained sufficient accurate or untainted evidence, the warrant is nevertheless valid." *Id.* at 954.

In the present case, probable cause did not exist, for the Naples Warrant, absent the illegally obtained information from the NIT search of the Defendant's computer. The test for determining probable cause is whether the facts presented to a judicial officer establish a fair probability that contraband or evidence of a crime will be found in a particular place. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The application for the Naples Warrant detailed how the I.P. address was linked to Mr. Caswell. It is clear that any probable cause determination hinged on the illegally obtained information from the search of the Defendant's computer. When removing the illegally obtained information, there is no remaining evidence present to establish any nexus to the address for which the Naples Warrant was sought and any likelihood that the items listed in the search warrant would be found in that particular location. The affidavit provided by the Government agent was clearly insufficient for the issuance of the Naples Warrant, given that it rested primarily on the illegally information obtained from the NIT search.

D. <u>The "Good Faith" exception does not apply.</u>

Federal agents could not have had a "good faith" belief that the NIT Warrant was in compliance with Rule 41(b). In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court recognized a good-faith exception to the exclusionary rule. In *Leon*, the Supreme

Court held that suppression was unwarranted where evidence was obtained pursuant to a search warrant that was later determined to be unsupported by probable cause, as the officers had a good-faith reliance on the warrant. *Levin,* 186 F.Supp.3d at 38. "None of the Supreme Court's post-*Leon* good-faith cases, however, involved a warrant that was void *ab initio*, and therefore none direct the conclusion that the good-faith exception ought to apply in this case." *Id.* at 39.

As a preliminary matter, federal agents could not have had a "good faith" belief that the NIT Warrant was in compliance with Rule 41(b). The federal agent who submitted the NIT Warrant application was a veteran agent who would have known the then-existing warrant jurisdictional limitations of Rule 41(b) and also known how a NIT worked. Further, the NIT Warrant application was submitted on February 20, 2015. Government agents should have been aware that a proposed amendment to Rule 41(b), to allow the exact NIT search at issue, had been proposed. The federal agent could not have had a good faith belief that then-existing Rule 41(b) justified the NIT Warrant and search of any user's computer.

The "good-faith" exception also does not apply, based on the particularity set forth in the NIT Warrant application and in the NIT Warrant itself, as to the place to be searched. The good-faith exception does not apply when "the magistrate or judge issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; or (2) "when a "warrant may be facially deficient—i.e., in failing to particularize the place to be searched or the thing to be seized—that the executing officers cannot reasonably presume it be valid." *Adams*, 2016

WL 421079, at 7. This case involves a reckless disregard for the truth in the NIT Warrant application, and a subsequent disregard for the NIT Warrant language. The federal agent, in the NIT warrant application, designated the place to be searched as the Government-controlled Playpen server in the Eastern District of Virginia. This was the exact place designated by the Virginia magistrate, as the place to be searched, in the NIT Warrant. So, there simply cannot be a good-faith belief of validity of the search, when the search occurs by infiltrating a user's computer in Florida.

Finally, the "good-faith" exception should not apply because the NIT Warrant was void *ab initio*. Some federal courts examining the Playpen website/NIT Warrant, have determined that a "good faith" exception should not apply in such a scenario. *Levin*, 186 F.Supp.3d at 38-42; Case No. 15-10271-WGY (D. Mass 2016); *Workman*, 2016 WL 5791209, at 7-8; *United States v. Arterbury*, No. 4:15-cr-00182-JHP, slip op. (N.D. Okla. April 25, 2016). The Defendant requests that the Court adopt the same reasoning and suppress the seized evidence.

II. THE DEFENDANT'S STATEMENTS SHOULD BE SUPPRESSED.

The Defendant's statements to federal agents should be suppressed, as the Defendant was subjected to custodial interrogation without the benefit of *Miranda* warnings.

1. The Requirements of the 5th Amendment.

The Fifth Amendment to the United States Constitution protects the right of persons to not be "compelled in a criminal case to be a witness against himself." U.S. Const. amend. V. A now basic legal requirement is that a subject be read *Miranda* rights prior to a

custodial interrogation. *See United States v. Brown*, 441 F.3d 1330, 1347 (11th Cir. 2006). While *Miranda* rights do not have to be read verbatim, the warnings read must convey the essential message that a defendant has the right to remain silent; that their statements may be used against them at trial; that they have the right to the presence of an attorney during questioning; and that, if they cannot afford a lawyer, one will be appointed to represent them. *California v. Prysock*, 453 U.S. 355 (1981). "It is by now undisputed that the right to Miranda warnings attaches when custodial interrogation begins." *Brown*, 441 F.3d at 1347.

2. "Custody" Defined.

The determination as to whether a defendant is "in custody", so as to require *Miranda* warnings before questioning, is objective and is made based upon the totality of the circumstances. *Stansbury v. California*, 511 U.S. 318, 323 (1994). "A defendant is in custody for the purposes of Miranda when there has been a "formal arrest or restraint on freedom of movement of the degree associated with a formal arrest." *Brown*, 441 F.3d at 1347. Even if a person has not been arrested, advice of *Miranda* rights is required if there is a restraint on freedom of movement of the degree associated with a formal arrest. *United States v. Muegge*, 225 F.3d 1267, 1270 (11th Cir. 2000).

In assessing custody, the issue is "...whether under the totality of the circumstances, a reasonable man in [the suspect's] position would feel a restraint on his freedom of movement to such extent that he would not feel free to leave." *Brown*, 441 F.3d at 1347. "The test is objective; the actual, subjective beliefs of the defendant and the interviewing officer about whether the defendant was free to leave are irrelevant." *Id.* The United States Supreme Court

has further explained that whether a defendant is in custody is an objective determination which required two discrete issues: (1) what were the circumstances surrounding the interrogation; and (2) given the circumstances, would a reasonable person have felt free to terminate the interrogation and leave. *J.D.B. v. North Carolina*, 564 U.S. 261, 270 (2011).

3. "Interrogation" Defined

The Miranda safeguards apply "whenever a person in is subjected to either express questioning or its functional equivalent." *Rhode Island v. Innis*, 446 U.S. 291, 300-301 (1980). The interrogation inquiry "refers not only to express questioning, but also to any words or actions on the part of the police (other than those normally attendant to arrest and custody) that the police should know are reasonably likely to elicit an incriminating response from the suspect." *Id.* at 301. The primary focus in determining whether an incriminating response was reasonably likely to be elicited from the suspect is on the perceptions of the suspect, rather than on the intent of the police. *Id.*

4. The Defendant's statements should be suppressed.

In the instant case, Mr. Caswell was subjected to custodial interrogation in the absence of Miranda warnings. Multiple federal agents, possibly ten or more, descended on the Defendant's home, in the early morning hours, to execute the search warrant. While Mr. Caswell's wife had already left for work, his children were still sleeping when federal agents arrived. Agents told Mr. Caswell that he was not under arrest and could leave; however, it is absurd to think that Mr. Caswell would have simply left his children sleeping in the house.

Agents questioned Mr. Caswell for well over an hour. During the interview, Mr. Caswell asked repeatedly to be able to call his wife; however, agents dismissed the request. At the end of the questioning, Mr. Caswell allegedly admitted to possessing child pornography. The agents never read Mr. Caswell *Miranda* warnings.

With regards to the issue of "custody", Mr. Caswell was in custody because a reasonable person in Mr. Caswell's position "would feel a restraint on his freedom of movement to such an extent that he would not feel free to leave." *Brown*, 441 F.3d at 1347. While the officers told Mr. Caswell that he could leave and did not have to speak with them, no reasonable person under the circumstances would perceive that they were free when confronted with multiple law enforcement officers searching the residence, repeated denial of access to a phone, and the unrealistic option of leaving children.

With regards to the issue of whether the questioning was an "interrogation", agents grilled Mr. Caswell for over an hour with questions that the agents knew were reasonably likely to elicit an incriminating response. Mr. Caswell was questioned regarding the occupancy of the house, Internet access, passwords, computers at the residence, and access to those computers. He was also questioned regarding the use of the TOR network and access to child pornography. The entire law enforcement questioning was for the purpose of eliciting incriminating responses from Mr. Caswell. Federal agents never told Mr. Caswell that he had the right to counsel, and that he had the right to confer with an attorney prior to answering any of the questions during the interrogation.

As a result, federal agents engaged in a custodial interrogation of Mr. Caswell, in violation of *Miranda*, 384 U.S. at 436. Had he been properly warned, Mr. Caswell would

have sought the advice of counsel instead of participating in the interrogation. Under the circumstances, all un-Mirandized statements and any fruits of un-Mirandized statements should be suppressed.

CONCLUSION

WHEREFORE, the Defendant requests that the Court suppress all evidence obtained as a result of the search and seizure stemming from the illegal NIT Warrant; all evidence obtained from the search and seizure stemming from the tainted Naples Warrant; and statements obtained from the Government's custodial interrogation of Mr. Caswell.

By: _____

Jerry Berry, Esquire
Attorney for Defendant
Florida Bar No. 288012
Law Offices of Jerry Berry, PA
2670 Airport Road South, Suite 300
Naples, Florida 34112
Telephone: (239)775-2255
Facsimile: (239) 775-6903
jberry@jberrylaw.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was filed electronically using ECF/CM with the Clerk of Courts Office and electronically provided to Charles D. Schmitz, United States Attorney's Office, c/o Charles.Schmitz@usdoj.gov on this 6th day of March, 2017.

By: _____

Jerry Berry, Esquire
Attorney for Defendant