UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

UNITED STATES OF AMERICA

v. CASE NO: 2:16-cr-134-FtM-29MRM

DAVID CASWELL
_____/

REPORT AND RECOMMENDATION

Pending before the Court is Defendant's Motion to Suppress Evidence (Doc. 17) filed on March 6, 2017.

Defendant's prosecution resulted from the Federal Bureau of Investigation's ("FBI") investigation of the child pornography website Playpen. Defendant is charged in a one-count indictment with knowingly possessing a matter that contained a visual depiction when the production of the visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction was of such conduct in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). (Doc. 3 at 1-2).

Defendant's Motion seeks to suppress certain evidence and statements. (Doc. 17 at 1). The Government filed a response (Doc. 22) to Defendant's Motion on March 20, 2017. The matter was referred to the Undersigned for a report and recommendation. The Undersigned conducted an evidentiary hearing on April 11, 2017.[1] The matter is ripe for review.

For the reasons set out herein, the Undersigned respectfully recommends that Defendant's Motion to Suppress Evidence (Doc. 17) be **DENIED**.

[1] A transcript of the proceedings is filed with the Court. (Doc. 34). The Undersigned cites to the Transcript of the April 11, 2017 evidentiary hearing as "Tr."

I. Evidence

The Government called two witnesses at the hearing: (1) FBI Special Agent Daniel Alfin, and (2) FBI Task Force Officer Kevin Bunch. (Tr. at 10, 64). The Government entered into evidence the following exhibits: a NIT[2] Search Warrant Application and Affidavit from the Eastern District of Virginia (Gov. Ex. 1); a local Search Warrant Application and Affidavit from the Middle District of Florida (Gov. Ex. 2); a CD containing an audio recording of an interview of David Caswell (Gov. Ex. 3); a transcript of the audio recording of an interview of David Caswell (Gov. Ex. 3t); and a CD containing a clip from the audio recording of an interview of David Caswell (Gov. Ex. 4). (*See* Doc. 29).

Defendant presented no witnesses and offered no evidence. The evidence and testimony were uncontroverted. Upon review, the Undersigned finds that the testimony of the witnesses was credible.

A. Witnesses

1. Special Agent Daniel Alfin

Special Agent Alfin has been employed as an FBI agent for eight years. (Tr. at 11:8-9). Agent Alfin is currently assigned to the criminal investigative division, violent crimes against children section, major case coordination unit at FBI headquarters. (*Id.* at 10-11). Agent Alfin's duties include "the investigation of individuals who used various types of technology to facilitate the production, distribution, advertisement, and possession of child pornography." (*Id.* at 11:2-5). Agent Alfin testified that he is trained in computer forensics and online investigative techniques for investigating child pornography offenses. (*Id.* at 12). Agent Alfin was involved in the investigation of the Playpen website from the beginning. (*Id.* at 40:18-19).

[2] As explained below, "NIT" is an acronym for Network Investigative Technique.

2. Task Force Officer Kevin Bunch

Officer Bunch is a detective with the City of Bradenton Police Department. (Tr. at 64:22-23). Officer Bunch has nineteen (19) years of experience with the Bradenton Police Department. (*Id.* at 65:10). Officer Bunch has been employed with the FBI's task force since 2012. (*Id.* at 64-65). Officer Bunch primarily handles child exploitation and cyber tips cases. (*Id.* at 65:17). Officer Bunch has training in interrogations and computer forensics. (*Id.* at 66). Officer Bunch was part of the team that executed the search warrant at Defendant's residence, and Officer Bunch also conducted an interview with Defendant at that time. (*Id.*).

B. The Tor Network

To discuss Defendant's case and the Playpen website, a discussion of the Tor network is required. "Tor" is an acronym for "The Onion Router." (Gov. Ex. 1, Doc. 29-2 at ¶ 7). "Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications." (*Id.*). The technology "is now available to the public at large." (*Id.*).

Agent Alfin testified that the Tor network "is a volunteer network of computers around the world." (*Id.* at 13:3-4). Agent Alfin also testified that the Tor network serves two primary purposes. (*Id.* at 13:4-5).

First, the Tor network allows users to access the regular Internet anonymously. (*Id.* at 13:6-7). Agent Alfin testified that browsing the Internet anonymously is the primary use of the Tor network. (*Id.* at 14:13-15). Agent Alfin testified that "[i]n the normal course of operation, when an individual accesses a website on the Internet, if they do it from their home here in Florida, when they access that website, that website will see their IP address." (*Id.* at 13:8-11).[3]

[3] "IP" is an acronym for Internet Protocol.

IP addresses are assigned to home Internet subscribers by Internet service providers ("ISP"). (*Id.* at 13:12-13). IP addresses can be used to identify users. (*Id.* at 13:15). Specifically, law enforcement can obtain a subpoena to request from an ISP the identity of an individual at a particular IP address at a given time. (*Id.* at 13:15-18). Agent Alfin testified that when users "access a website normally, the website can see and record your IP address," thus making it possible to identify an individual that accesses a website. (*Id.* at 13:19-22).

The Tor network, however, enables users to browse the Internet anonymously. (*Id.* at 14:13-14). When users connect to the Tor network, a user's Internet traffic "is now generally being routed through three different computers almost anywhere in the world" instead of "connecting directly to a website." (*Id.* at 13:23 – 14:2). The computers that route traffic on the Tor network are known as "nodes." (*Id.* at 17:18). When connecting to a regular Internet website via the Tor network, a user's traffic travels through three different Tor nodes—the "entry guard node," a "middle node," and an "exit node." (*Id.* at 19:3-7). A user's true IP address must be transmitted to the entry guard node. (*Id.* at 19:15). The entry guard node is generally randomly assigned by the Tor software. (*Id.* at 19:24-25). The Tor software is able to protect a user's privacy by "bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user." (Gov. Ex. 1, Doc. 29-2 at ¶ 8).[4] The user's traffic eventually leaves though an exit node—*i.e.*, the last computer through which a user's communications were routed. (*Id.*). When a user on the Tor network accesses a website, that website logs the IP address of the exit node, not the user's actual IP address. (*Id.*). Agent Alfin

[4] Agent Alfin testified that "[a]nyone who wants to can download the Tor software, install it on their computer, and become a node in the Tor network. And by doing so, you have now added your computer . . . to the Tor network." (Tr. at 17:20-24).

testified that this process allows users to access the desired website, but the website will not be able to know where the user is located. (Tr. at 14).

The second use of the Tor network is "hidden services." (*See id.* at 14). Agent Alfin testified that Tor hidden services applies the same anonymity concepts afforded to browsing to the end website. (*Id.*). By way of example, Agent Alfin testified that for a regular website such as CNN.com, it is possible "to use any number of publicly available databases to see the true IP address of CNN.com," including who owns the website and where the website is hosted. (*Id.* at 14:20-23). Websites set up as Tor hidden services, however, force connections to that website to go through the Tor network. (*Id.* at 15:1-3). As a result, there are "six Tor network servers between the end user and the Tor hidden service," thereby anonymizing the actual location of the website. (*Id.* at 15:3-7). Agent Alfin stated that the location of Tor hidden service websites are unknown. (*Id.* at 15:10). The website could be located "in the same room that I'm in, or it could be in Germany, or it could be almost anywhere else in the world" because it is not possible to see the website's true IP address, nor can the website see a user's true IP address. (*Id.* at 15:10-15).

Agent Alfin testified that the Tor network allows creators "to put whatever content you want" on hidden services websites because although law enforcement can access the website, "there's not much we can do about it" because law enforcement does not know where the website is located. (*Id.* at 15-16). Agent Alfin testified that another benefit to the Tor network is that traffic on the Tor network is encrypted. (*Id.* at 18:4-5). Encryption prevents data sent on the network from being usable or readable by law enforcement. (*Id.* at 18:18-20).

Additionally, Agent Alfin testified that Tor hidden services websites are configured differently than regular websites. (*See id.* at 21). For regular websites, the Uniform Resource Locator ("URL") – the human readable name for the website – "looks like CNN.com, or

Google.com." (*Id.* at 21:22-25). For a Tor hidden services website like Playpen, however, the URLs are generally 16 random characters assigned when the Tor hidden services website is created. (*Id.*). In addition, the website ends with the suffix ".onion" and not a common suffix such as ".com" or ".org." (*Id.* at 22:1-4).

To access a Tor hidden services website, users must utilize a web browser specifically configured to access the Tor network. (*Id.* at 22:5-7). Further, due to the anonymizing features of the Tor network, "[i]t takes a little bit of effort" to find hidden services websites. (*Id.* at 24:5). Users may locate Tor hidden services websites via "various index sites that exist within the Tor network as their own hidden services." (*Id.* at 22:12-13). Alternatively, it is possible to learn of Tor hidden services websites from other users. (*Id.* at 23:18). Due to the steps required to access Tor hidden services websites, Agent Alfin testified that it is incredibly unlikely that someone would find their way to a hidden services website like Playpen accidentally. (*Id.* at 22:22-23).

C. The Playpen Website

Agent Alfin testified that "in approximately August 2014, the Playpen website came online in the Tor network." (Tr. at 16:4-6). Agent Alfin learned about the existence of Playpen from an index website that maintains up-to-date lists of active child pornography websites. (*Id.* at 22). Agent Alfin observed that Playpen "was a website dedicated to the advertisement and distribution of child pornography" and "had hundreds of thousands of members." (*Id.* at 16:7-10). Agent Alfin testified that everything on the website revolved around child pornography and child exploitation, including the posting of images and videos and a discussion on how to keep child pornography collections encrypted. (*Id.* at 17).

While Agent Alfin could access the site, the FBI was unable to determine its location due to the nature of the Tor network. (*Id.* at 16:11-17). In December 2014, however, the FBI

discovered that the Playpen website was misconfigured. (*Id.* at 20). At that time, although Playpen users were cautioned not to use a real email address when creating a Playpen account, if users created an account with an actual email address, the Playpen website sent an email confirming the account registration. (*Id.* at 21). That confirmation email contained the actual IP address of the Playpen website. (*Id.*). This misconfiguration allowed the FBI to determine that the Playpen website was located in North Carolina. (*Id.* at 21:17).[5] Eventually, using various forms of legal process, the FBI was able to locate the owner and creator of the Playpen website at a location in Naples, Florida. (*Id.* at 25). Notwithstanding these developments, the FBI was still unable to investigate the users of Playpen because users accessed the website though the Tor network. (*Id.* at 26).

On February 20, 2015, the FBI took administrative control of the Playpen website. (*Id.* at 26-27). The hard drives of the website's server in North Carolina were seized as evidence and a copy of the website was transferred to a Government facility in the Eastern District of Virginia. (*Id.* at 27). To investigate the site's users, the Government operated the Playpen website for a period of thirteen (13) days – from February 20, 2015 to March 4, 2015 – at a Government facility in the Eastern District of Virginia. (*Id.*). During that time, the FBI did not upload any content to the website, but instead allowed the website to operate normally. (*Id.* at 28). The Government did, however, track users' activity during that time. (*Id.*).

D. The NIT Warrant

On February 20, 2015, the FBI obtained a warrant ("NIT Warrant") to utilize a procedure known as the Network Investigative Technique ("NIT"). (*Id.* at 28; *see also* Gov. Ex. 1, Doc.

[5] An additional misconfiguration in the website was later discovered that allowed the FBI to access Playpen over the regular Internet. (Tr. at 24).

29-2). An Application for a Search Warrant was submitted by FBI Special Agent Douglas Macfarlane to United States Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. (Gov. Ex. 1, Doc. 29-2 at 2). The Affidavit in Support of Application for Search Warrant stated the relevant statutes, provided definitions to relevant terms, and described – in explicit detail – why probable cause existed. (*See id.* at 6-36).

In the Affidavit, Agent Macfarlane described what the NIT was and why it was necessary. (*Id.* at 28). The Affidavit stated that normally, "websites send content to visitors." (*Id.* at ¶ 33). Agent Macfarlane stated that "[a] user's computer downloads that content and uses it to display web pages on the user's computer." (*Id.*). Agent Macfarlane wrote that the NIT – located in the Eastern District of Virginia – would augment that content "with additional computer instructions." (*Id.*). Specifically, when a Playpen user's computer successfully downloaded the additional instructions from the Playpen website, the instructions were designed to cause the "activating computer" to transmit certain information to a Government-controlled computer. (*Id.*). Attachment B of the Application stated that the specific "Information to be Seized" from an "activating computer." (*Id.* at 38). This information included:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

2. a unique identifier generated by the NIT (*e.g.*, a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers, that will be sent with and collected by the NIT;

3. the type of operating system running on the computer, including type (*e.g.*, Windows), version (*e.g.*, Windows 7), and architecture (*e.g.*, x 86);

4. information about whether the NIT has already been delivered to the "activating" computer;

5. the "activating" computer's Host Name;

6. the "activating" computer's active operating system username; and

7. the "activating" computer's Media Access Control ("MAC") address.

(*Id.*). Agent Macfarlane wrote that "the NIT will not deny the user of the 'activating' computer access to any data or functionality of the user's computer." (*Id.* at ¶ 33).

Attachment A of the Application defined "activating computers" as any computer "of any user or administrator who logs into [Playpen] by entering a username and password." (*Id.* at 37). In the Affidavit, Agent Macfarlane specifically requested authority to use the NIT "to investigate any user or administrator who logs into [Playpen] by entering a username and password." (*Id.* at ¶ 32). Additionally, the Affidavit specifically requested that the NIT Warrant authorize the NIT to cause "an activating computer – wherever located – to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location other information about the computer and the user of the computer, as described above and in Attachment B." (*Id.* at ¶ 46(a)).

Agent Macfarlane wrote that – due to the nature of the Tor network – the NIT was necessary "to locate and apprehend [subjects] who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation." (*Id.* at ¶¶ 30-31).

Judge Buchanan authorized the search warrant and commanded its execution on or before March 6, 2015. (*Id.* at 3).

Agent Alfin testified at the hearing that the NIT was computer code installed on a Government server in the Eastern District of Virginia where the Government was running the Playpen website. (Tr. at 31). Agent Alfin testified that the purpose of the NIT was to determine a user's actual IP address. (*Id.*). Agent Alfin testified that but for a user's conduct, the NIT would have remained dormant on the server in the Eastern District of Virginia. (*Id.*). Agent

Alfin testified that when users requested information from the Playpen website, the NIT code was attached to that information and traveled to that user's computer – wherever the computer may have been located – and forced the computer to send to the Government "the real IP address of the computer, along with a minimal amount of other identifying information." (*Id.* at 30:16-22). Specifically, the NIT code forced the user's computer to briefly communicate outside of the Tor network with a Government server in the Eastern District of Virginia. (*Id.* at 31:18-21). In doing so, the Government was able to see "the real IP address of the computer, not the one that the Tor network presents." (*Id.* at 31:21-23).

Agent Alfin testified that all of the information sought by the NIT was aimed at determining the final location of the NIT. (*Id.* at 34:22-23). Agent Alfin testified that the IP address was the most valuable piece of information because it can be used to identify a physical address. (*Id.* at 35-36). Agent Alfin testified, however, that an IP address resides on a modem, not on any particular computer. (*Id.* at 36). As such, the IP address of a computer changes when it connects to the Internet via a different network. (*See id.*). For instance, if a computer is taken from a house to a Starbucks, then the IP address of the computer will reflect the IP address of the wireless router at Starbucks, not the IP address associated with the modem at the house. (*Id.* at 37). Agent Alfin testified that the rest of the information sought by the NIT was designed to determine the specific device and user among the various potential devices and users that may be associated with a particular IP address. (*Id.* at 35).

The NIT operated quickly—usually in less than one second. (*Id.* at 31-32). Agent Alfin testified that nothing remained on the user's computer after the NIT finished its operation. (*Id.* at 32). Agent Alfin further testified that nothing was installed on an end user's computer. (*Id.* at 37). The FBI had no ability to access the computer again after the NIT performed its operation.

(*Id.* at 39). Instead, Agent Alfin testified that the NIT executed various functions by "go[ing] in and gather[ing] information." (*Id.* at 51). The NIT pulled active information from the computer's system memory. (*Id.* at 52).

Additionally, Agent Alfin testified that users had to perform several steps to cause the NIT to perform its operation. (*Id.* at 47). First, a user had to log in with a user name and password to the Playpen website. (*Id.*). Once on the site, Agent Alfin testified that the NIT generally performed its operation only when a user clicked on one of the various sub-forums off of the main index page. (*Id.*).

Agent Alfin testified that he disagreed with the NIT being described as "malware." (*Id.* at 32).[6] Agent Alfin conceded, however, that Playpen users "would not want the NIT on their computer." (*Id.* at 46). Agent Alfin testified that users of the Tor network are trying to conceal their IP addresses and are hoping that no one will obtain their true IP address. (*Id.* at 44).

Agent Alfin testified that he had been involved with the Playpen investigation from the beginning. (*Id.* at 40). Agent Alfin further testified that he had no reason to believe the NIT Warrant was invalid. (*Id.*). Agent Alfin testified that he worked closely with Department of Justice ("DOJ") attorneys, lawyers in the FBI Office of General Counsel, and other FBI agents who reviewed the NIT Warrant. (*Id.*). It was Agent Alfin's understanding that the warrant was properly issued. (*Id.* at 41). In coming to that conclusion, Agent Alfin relied on the opinions of Government lawyers. (*Id.*).

E. Naples Search Warrant and Interview of Defendant

Using the NIT, FBI Task Force Agent Zachary Ewert stated that Defendant or a user of the Internet account "WhaddupYall" at Defendant's address in Naples, Florida accessed the

[6] "Malware" is short for malicious software. (Tr. at 32).

Playpen website. (Gov. Ex. 2, Doc. 29-3 at 11 ¶¶ 6, 31). Agent Ewert stated in his Affidavit in Support of Search Warrant that user "WhaddupYall" was actively logged into Playpen for fifteen (15) hours between January 26, 2015 and March 4, 2015. (*Id.* at ¶ 32). Using the logs from the website and the NIT, Agent Ewert stated that "WhaddupYall" accessed images on Playpen from IP address 76.101.22.195 on February 26, 2015. (*Id.* at ¶ 33). Additionally, on March 2, 2015 and March 4, 2015, the user account "WhaddupYall" accessed other images, but the IP address was not collected on those occasions. (*Id.* at ¶¶ 35-37). Using an administrative subpoena, the FBI discovered that Defendant was receiving Internet service associated with the above IP address. (*Id.* at ¶ 39). Based on the information contained in the Application, the Undersigned authorized a search warrant ("Naples Search Warrant") at Defendant's residence. (*Id.* at 1). Agents executed the search warrant on August 6, 2015. (*See* Gov. Ex. 3t, Doc. 29-5 at 1).

Officer Bunch testified at the hearing that he was part of the team that executed the Naples Search Warrant. (Tr. at 68). Additionally, Officer Bunch conducted an interview with Defendant. (*Id.* at 66). Officer Bunch testified that the search occurred at 6:00 a.m. (*Id.* at 69:12). Officer Bunch testified that agents came to Defendant's front door, knocked, and rang the doorbell. (*Id.* at 68-69). Defendant met the agents at the door. (*Id.* at 68). Six or seven agents executed the warrant. (*Id.* at 77). The agents were wearing bullet-proof vests. (*Id.*). The agents explained who they were and that they had a search warrant. (*Id.* at 68). After Defendant stepped out of his residence, the agents then entered the home. (*Id.*). When the agents entered Defendant's home, their firearms were drawn for safety purposes. (*Id.* at 78). Defendant's children were present during the search but remained sleeping in their bedrooms. (*Id.* at 69:1-3).

Officer Bunch testified that he asked to speak with Defendant. (*Id.* at 69-70). Defendant agreed to speak with the agents. (*Id.* at 70). Officer Bunch and Agent Ewert conducted the

interview. (*Id.* at 70:3-4). The interview occurred on the back patio of Defendant's residence next to the pool. (*Id.* at 70:7-8). The officers' guns were not drawn during the conversation. (*Id.* at 70:11). Officer Bunch testified that Defendant was not allowed to enter his residence for safety reasons. (*Id.* at 74). Defendant was wearing a t-shirt and shorts. (*Id.* at 70:15).

Officer Bunch testified that his interviews are light-hearted, relaxed, and voluntary. (*Id.* at 70:21-22). Officer Bunch testified that Defendant was instructed that he was under no obligation to talk to the agents and that he could leave with his children at any time. (*Id.* at 74-75). The transcript of the interview shows the following exchange:

> KB: [] you understand you're not under arrest, correct?
>
> DC: Yeah.
>
> KB: Okay. You could leave at any time. And anytime, you can stop talkin' to -- you can say, "Bunch, Zac, I'm done talkin' to you – "
>
> DC: I watch the shows.
>
> KB: – it – and walk away. No, just so you understand.
>
> DC: No problem.
>
> KB: Um, and so if – but, because we're doin' a search warrant, we gotta limit where you go in the house. So if you wanna walk out your lanai, hop the fence and go, I'll wave to ya.
>
> DC: That's fine.
>
> KB: But I mean, uh, when it's somethin' with the kids, yeah, we – we – we wanna do it very – we wanna make sure that the kids aren't scared, or anything like that.
>
> DC: All right.
>
> KB: Uh, so – but if you have to get up, let me know. Or if you wanna leave, let me know.

(Gov. Ex. 3t, Doc. 29-5 at 4).

After the interview and search were complete, the agents left. (Tr. at 75). Defendant was not placed under arrest at that time. (*Id.*).

II. Analysis

Defendant seeks to suppress three types of evidence. First, Defendant seeks to suppress evidence obtained as a result of the NIT Warrant on the ground that the information was obtained by an illegal search of Defendant's computer in violation the Fourth Amendment, 28 U.S.C. §636(a), and Fed. R. Crim. P. 41. (Doc. 17 at 1). Second, Defendant argues that the evidence obtained from the search of his residence should be suppressed because the Naples Search Warrant was tainted by the NIT Warrant. (*Id.*). Finally, Defendant seeks to suppress all statements obtained by the Government at his residence on the basis that the Government failed to give him *Miranda* warnings. (*Id.*).[7] The Undersigned addresses each of these arguments in turn.

A. The NIT Warrant

The FBI's investigation of Playpen has resulted in numerous prosecutions around the country. As a result of these prosecutions, the NIT Warrant has been challenged in dozens of cases nationally. As such, many of Defendant's arguments regarding the NIT Warrant are similar or identical to those made in other jurisdictions. Defendant specifically argues that suppression is warranted here because (1) the NIT Warrant violated the Fourth Amendment and/or (2) the NIT Warrant violated 28 U.S.C. §636(a) and Fed. R. Crim. P. 41.

Before addressing the specific issues raised by Defendant's Motion regarding the NIT Warrant, the Undersigned notes that this Court recently addressed virtually identical issues relating to the NIT Warrant in *United States v. Hart*, No. 2:16-cr-110-FTM-29CM, slip op. Doc.

[7] *Miranda v. Arizona*, 384 U.S. 436 (1966).

50 (M.D. Fla. Apr. 27, 2017), *report and recommendation adopted*, No. 2:16-cr-110-FTM-29CM, 2017 WL 2822747 (M.D. Fla. June 30, 2017). In *Hart*, the Honorable John E. Steele, the presiding district judge in this case, accepted and adopted United States Magistrate Judge Carol Mirando's Amended Report and Recommendation in full. 2017 WL 2822747, at *2. In doing so, the Court found that the NIT Warrant was validly issued and, therefore, denied the defendant's motion to suppress on this ground. *See id.* Similarly, here, because Judge Steele accepted and adopted Judge Mirando's conclusions of law and because the record relating to the NIT Warrant in this case is virtually identical to the record developed in *Hart*, the Undersigned finds and recommends that Defendant's Motion to Suppress be denied on this ground.

1. Compliance with the Fourth Amendment

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their person, 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 particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

The text of the constitution provides two basic requirements. First, "all searches and seizures must be reasonable." *Kentucky v. King*, 563 U.S. 452, 459 (2011). "[R]easonableness generally requires the obtaining of a judicial warrant." *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). Second, "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *King*, 563 U.S. at 459. In addition to the textual requirements, the Supreme Court has stated that warrants must be issued by a neutral, disinterested magistrate. *Dalia v. United States*, 441 U.S. 238, 255 (1979).

The Fourth Amendment's protection, however, is only implicated when "the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citations and internal quotation marks omitted). A person claiming a violation of the Fourth Amendment must demonstrate that he or she has an actual, subjective expectation of privacy. *Id.* Moreover, that subjective expectation of privacy must be one that society is prepared to recognize that expectation as reasonable. *Id.*

Defendant argues that the Fourth Amendment is implicated because he had a reasonable expectation of privacy in his computer. (Doc. 17 at 6). Defendant then argues that his Fourth Amendment rights were violated because the NIT Warrant failed to properly designate the particular pace to be searched. (*Id.*). Defendant contends that the NIT Warrant authorized a search to occur on the Playpen server in the Eastern District of Virginia, but the actual search of Defendant's computer occurred in Florida. (*Id.* at 8).

The Court need not address whether the Fourth Amendment is implicated here based on a reasonable expectation of privacy in the contents of Defendant's computer because even if the Fourth Amendment is implicated, Defendant has not shown a violation of the Fourth Amendment. Defendant's sole contention that the NIT Warrant violated the Fourth Amendment is based on the particularity requirements. Defendant does not argue that the other requirements of the Fourth Amendment were not met—*i.e.*, that the NIT Warrant was not supported by probable cause or that it was not issued by a neutral and disinterested magistrate judge. *See King*, 563 U.S. at 459; *Dalia v. United States*, 441 U.S. at 255.

With regard to the particularity requirements of the Fourth Amendment, the Eleventh Circuit has noted that a warrant's description of the place to be searched only requires "sufficient

particularity to direct the searcher, to confine his examination to the place described, and to advise those being searched of his authority." *United States v. Burke*, 784 F.2d 1090, 1092 (11th Cir. 1986); *see also United States v. Rousseau*, 628 F. App'x 1022, 1025 (11th Cir. 2015). Similarly, a description of the materials to be seized "is sufficiently particular when it enables the searcher reasonably to ascertain and identify the things to be seized." *United States v. Santarelli*, 778 F.2d 609, 614 (11th Cir. 1985); *see also Rousseau*, 628 F. App'x at 1025. The Eleventh Circuit has noted that "[e]laborate specificity is unnecessary." *U.S. v. Strauss*, 678 F.2d 886, 892 (11th Cir. 1982).

Other courts reviewing the NIT Warrant have addressed this precise issue. It appears that most, if not all, of the courts that have considered the issue have found that the particularity requirements of the Fourth Amendment are met by the NIT Warrant. *See, e.g.*, *Taylor*, No. 2:16-cr-00203-KOB-JEO-1, 2017 WL 1437511, at *11 (N.D. Ala. Apr. 24, 2017).

For instance, in *United States v. Taylor*, the court found that the NIT Warrant was sufficiently particular. 2017 WL 1437511, at *11. There, the court noted that Attachments A and B to the Warrant were correctly incorporated into the NIT Warrant by reference. *Id.* The court found that "Attachments A and B clearly identified the 'place' to be searched (the NIT would be deployed to the computer server in the Eastern District of Virginia and then to computers logging into the Playpen website) and the information to be seized (Attachment B includes an itemized list of the seven pieces of information to be seized)." *Id.* The court noted that "[t]hough the Constitution does not require elaborate specificity, the court finds it difficult to imagine how much more specific the descriptions of the place to be searched and the items to be seized could have been." *Id.* Thus, the court held that the NIT Warrant was sufficiently particular. *Id.*

After an independent review in this case, the Undersigned finds that the NIT Warrant clearly describes the place to be searched—*i.e.*, Attachments A and B clearly identified the 'place' to be searched (the NIT would be deployed to the computer server in the Eastern District of Virginia and then to computers logging into the Playpen website). (*See* Gov. Ex. 1, Doc. 29-2 at 37-38). Moreover, the NIT Warrant explicitly states the items to be seized—*i.e.*, Attachment B includes an itemized list of the seven types of information from the activating computers. (*Id.* at 38). As noted by the Court in *Taylor*, while the Constitution does not require elaborate specificity, the Undersigned finds "it difficult to imagine how much more specific the descriptions of the place to be searched and the items to be seized could have been." 2017 WL 1437511, at *11. Thus, the Undersigned finds that the NIT Warrant satisfies the Fourth Amendment's particularity requirements.

Because the NIT Warrant complies with the Fourth Amendment, the Court need not address Defendant's other contention that he had a reasonable expectation of privacy in the contents of his personal computer such that the Fourth Amendment is implicated. Assuming, *arguendo*, that the Fourth Amendment is implicated, there was no violation of the Fourth Amendment. Defendant's Motion to Suppress (Doc. 17) should, therefore, be denied on this ground.

2. Whether the NIT Warrant Violated Federal Rule of Criminal Procedure 41(b) and/or the Federal Magistrates Act

In addition to the constitutional challenge, Defendant also challenges the NIT Warrant for an alleged violation of the Federal Magistrates Act and Federal Rule of Criminal Procedure 41(b).

The Federal Magistrates Act, 28 U.S.C. § 636(a), provides:

> Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge . . . (1) all powers and duties conferred or imposed upon United States commissioners or by law or by the Rules of Criminal Procedure for the United States District Courts.

Federal Rule of Criminal Procedure 41(b) confers upon magistrate judges the authority to issue warrants. Accordingly, because the Federal Magistrates Act, 28 U.S.C. § 636(a) provides that United States magistrate judges have "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure," the question of whether the Federal Magistrates Act was violated turns on whether the NIT Warrant violated the Federal Rules of Criminal Procedure. *See Taylor*, 2017 WL 1437511, at *12.

At the time the NIT Warrant was issued in 2015, Rule 41(b) allowed magistrate judges to issue warrants in five circumstances. *See also Adams*, 2016 WL 4212079, at *5. Defendant argues that the NIT Warrant was invalid under Rule 41(b)(1), (2), and (4). (Doc. 17 at 9-15). The Government, however, only argues that the NIT Warrant was properly authorized pursuant to Fed. R. Crim. P. 41(b)(4). (*See* Doc. 22 at 11). Thus, if the NIT Warrant was properly authorized under Rule 41(b)(4), then the Court need not address Rule 41(b)(1) or (2) in the alternative.

Fed. R. Crim. P. 41(b)(4) allows magistrate judges to issue warrants for the installation of a "tracking device." Specifically, Fed. R. Crim. P. 41(b)(4) provides that "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 the device to track the movement of a person or property located within the district, outside the district, or both." "Property" is defined by Fed. R. Crim. P. 41(a)(2)(A) as including "documents, books, papers, any other tangible objects, and information." Fed. R. Crim. P. 41(a)(2)(E) defines a "tracking device" as having "the

meaning set out in 18 U.S.C. § 3117(b)." That statute defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

A review of Fed. R. Crim. P. 41(b)(4) shows that the Court must consider three basic requirements of the Rule in relation to the NIT authorized by the NIT Warrant. First, the Court must determine whether the NIT is a "tracking device." Second, the Court must evaluate whether the tracking device was "installed" within the relevant district. Finally, the Court must evaluate whether the device "tracked" the movement of a person or property or whether it did something else—such as perform a search. *See id.*

Before addressing the specific issues raised by Defendant's Motion, the Undersigned notes that many courts have addressed this precise issue regarding the same NIT Warrant and its relationship to the Federal Magistrates Act and Fed. R. Crim. P. 41. The decisions of these courts fall into four general categories.

First, a number of courts – including this Court recently in *Hart* – have determined that the NIT Warrant did not violate the Federal Magistrates Act and/or Rule 41 and, therefore, denied the motions to suppress. *See Hart*, No. 2:16-cr-110-FTM-29CM, slip op. Doc. 50 at 19-21.[8] *See also, e.g.*, *United States v. Jean*, 207 F. Supp. 3d 920, 938 (W.D. Ark. 2016); *United States v. Matish*, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016); *United States v. Darby*, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016).

[8] As noted above, Judge Mirando's Amended Report and Recommendation in *Hart* was accepted and adopted by the Court in full. 2017 WL 2822747, at *2. Because Judge Mirando's analysis represents the opinion of the Court, the Undersigned cites to the page numbers of the Amended Report and Recommendation for ease of reference here.

Second, other courts – including this Court in *Adams* and in *United States v. Kneitel* – have determined that the NIT Warrant violated the Federal Magistrates Act and/or Rule 41 but, nevertheless, determined that suppression was not warranted. *See Adams*, 2016 WL 4212079, at *6; *United States v. Kneitel*, 8:16-cr-0023-MSS-JSS, slip op. at Doc. 158 at 2 (M.D. Fla. Jan. 3, 2017). *See also, e.g.*, *Taylor*, 2017 WL 1437511, at * 14; *United States v. Werdene*, 188 F. Supp. 3d 431, 442 (E.D. Pa. 2016).

Third, still other courts have declined to decide the issue of whether the Federal Magistrates Act and/or Rule 41 were violated but, nevertheless, found that suppression was not warranted. *See, e.g., United States v. Schuster*, No. 1:16-CR-51, 2017 WL 1154088, at *5-6 (S.D. Ohio Mar. 28, 2017); *United States v. Tran*, No. CR 16-10010-PBS, 2016 WL 7468005, at *5-6 (D. Mass. Dec. 28, 2016).

Finally, a minority of courts have determined that the NIT Warrant violated Rule 41(b) and found that suppression was warranted. *See United States. v. Croghan*, 209 F. Supp. 3d 1080, 1093 (S.D. Iowa 2016); *United States v. Workman*, 205 F. Supp. 3d 1256, 1269 (D. Colo. 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, slip op. Doc. 47 at 1 (N.D. Okla. May 12, 2016) (adopting magistrate judge's report and recommendation); *United States v. Levin*, 186 F. Supp. 3d 26, 44 (D. Mass. 2016).

Here, the Government argues that the NIT Warrant was properly authorized as a tracking device pursuant to Fed. R. Crim. P. 41(b)(4). (Doc. 22 at 11). The Government points out that the definition of "property" within the Rule applies not only to tangible property (such as a stolen vehicle) but also intangible property (such as electronic information). (*Id.* (citing Fed. R. Crim. P. 41(a)(2))). The Government argues that the NIT tracked Defendant's information. (*See id.*).

The Government further argues that the NIT properly complied with the other requirements of the Rule. (*See id.*). For instance, the Government argues that the NIT was properly installed in the Eastern District of Virginia. (*Id.* at 13). Specifically, the Government argues that the NIT code was installed on the server in the Eastern District of Virginia and that, but for the Defendant's actions, the NIT would have remained dormant in the Eastern District of Virginia. (*Id.*). The Government contends that Defendant reached into the Eastern District of Virginia and took the NIT, along with the content of the Playpen website, back with him to Florida. (*Id.*). The Government argues that the fact that the NIT performed its operation in Florida does not change the location of where the NIT was installed. (*Id.* at 14).

Additionally, the Government argues that the NIT tracked, not searched. (*Id.* at 16). The Government specifically argues that the NIT is a tracker because it only obtained location information. (*Id.*). The Government contends that "[n]ot only did the NIT track the child pornography files to the defendant's physical address (through the defendant's IP address), but it also tracked the child pornography to a specific computer within that address that ran the defendant's operating system, and contained the defendant's username and MAC address." (*Id.* at 17-18). The Government argues that "just like a standard tracking device, all information that the tracker caused to be sent to the FBI was location information." (*Id.* at 18).

Finally, the Government argues that because the NIT Warrant was validly issued pursuant to Rule 41(b)(4), the Federal Magistrates Act was not violated. (*See id.* at 13-20). Specifically, the Government argues that the NIT Warrant does not violate the Federal Magistrates Act because it was duly authorized by Judge Buchanan within the powers conferred upon her by the Federal Rules of Criminal Procedure. (*Id.* at 20). Even if Rule 41 was violated, however, the Government argues that suppression is not an appropriate remedy. (*Id.*).

For his part, Defendant contends that the NIT Warrant violates Rule 41(b)(4). (Doc. 17 at 13). Specifically, Defendant argues that the NIT Warrant is invalid under the Rule because the NIT was installed in Florida, not Virginia. (*Id.* at 14). Moreover, Defendant argues that even if the NIT was installed in Virginia, the NIT violates Rule 41(b)(4) because it searches instead of tracks. (*Id.*). Defendant argues that suppression is an appropriate remedy under the circumstances as a result of the violation of Rule 41(b). (*Id.* at 15).

As stated above, the courts that have addressed the same or similar arguments have arrived at varying conclusions as to whether the NIT violated Rule 41(b)(4).

Notably, this Court found in *Hart* that Magistrate Judge Buchanan properly issued the NIT Warrant pursuant to Fed. R. Crim. P. 41(b)(4). *Hart*, No. 2:16-cr-110-FTM-29CM, slip op. Doc. 50 at 19-21. The Court specifically rejected the defendant's arguments that the NIT was installed on the defendant's computer in Florida and that the defendant never "controlled" the government-controlled computer. *Id.* at 19. The Court stated:

> While it is true that neither Defendant nor his computer physically traveled to Virginia, it is equally true that the FBI did not physically travel to Florida to install the NIT in Defendant's computer. The FBI installed the NIT in the Eastern District of Virginia by augmenting the content on the Playpen website with additional computer instructions comprising the NIT. Those computer instructions transmitted electronically over the Internet to track the movement of property — in this case, intangible "information," appearing as content on the Playpen website. Although Defendant focuses on the location of his computer, in order to become an activating computer, it is undisputed that Defendant had to log into the Playpen website, which was located in the Eastern District of Virginia, and voluntarily download content from that website. Thus, Defendant's voluntary actions of "virtually" visiting the Eastern District of Virginia and downloading the NIT, which was embedded in the Playpen content, caused the NIT to travel to Defendant's computer located in Florida. Accordingly, but for Defendant's voluntary actions, the NIT would have remained dormant in the Eastern District of Virginia and never deployed in the Defendant's computer in Florida.

Id.

The Court in *Hart* cited several other court decisions that endorsed the "virtual trip" theory. *Id.* at 20-21 (citing *United States v. Sullivan*, No. 1:16-CR-270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); *United States v. Lough*, 221 F. Supp. 3d 770, 778 (N.D. W. Va. 2016); *Matish*, 193 F. Supp. 3d at 612-13; *Darby*, 190 F. Supp. 3d at 536). Additionally, the Court noted that "after the NIT completed its function, which Agent Alfin testified generally was within 'less than a second,' it disappeared from Defendant's computer without a trace." *Id.* at 20. The Court found that the NIT "did not make any changes to Defendant's computer" nor did it "provide the FBI the ability to access Defendant's computer." *Id.*

The Court in *Hart* acknowledged the fact that other courts – including a decision of this Court in *Adams* – had rejected "the idea of a virtual tracking device" on the ground that "the NIT did not obtain the website user's IP address by tracking information but did so by searching the user's computer." *Id.* at 21 (citing *Adams*, 2016 WL 4212079, at *6). Nevertheless, *Hart* found this rationale to be unpersuasive. *Id.* Instead, the Court found "that the NIT did not search but tracked information as contemplated by 41(a)(2)(A)." *Id.* Additionally, the Court found that "the NIT would not have been deployed in Defendant's computer but for Defendant's actions." *Id.* Thus, the Court found that the NIT Warrant was validly issued pursuant to Fed. R. Crim. P. 41(b)(4). *See id.*

Similarly, the court in *Darby* found that Rule 41(b)(4) gave the magistrate judge authority to issue the NIT Warrant. 190 F. Supp. 3d at 536. There, the court found that Playpen users "digitally touched down in the Eastern District of Virginia when they logged into the site." *Id.* The court stated that when the users logged in, the Government placed the NIT code on their home computers, which may have been outside of the district, and sent information to the Government regarding the user's location. *Id.* The court noted that Rule 41(b)(4) allows

magistrate judges to issue a warrant for a tracking device to be installed in the magistrate judge's district and that "the tracking device may continue to operate even if the object tracked moves outside the district." *Id.* The court found that the NIT did exactly that function and found, therefore, that Judge Buchanan did not violate Rule 41(b)(4) in issuing the NIT Warrant. *Id.*

An additional example can be found in *Jean*, 207 F. Supp. 3d at 941. There, the Court determined that the NIT Warrant was properly issued pursuant to Rule 41(b)(4). *Id.* at 943. In making that determination, the court specifically analyzed whether the NIT could be considered a "tracking device." *See id.* The court noted that the term "device" is a word commonly used to describe "a tool or *technique* used to do a task." *Id.* (citation omitted). The court found that the NIT was a tracking device pursuant to Rule 41(b)(4) because (1) the NIT was an electronic device within the meaning of 18 U.S.C. § 3117(b) as it was "an investigative tool consisting of computer code transmitted electronically over the internet" and (2) the purpose of the NIT was to track the movement of "property," specifically "intangible information," which definition of "property" is contemplated by Rule 41(a)(2)(A). *Id.* at 942.

As to the installation of the device, the court noted that the term "install" was problematic. *Id.* The court noted that while it was true that the defendant and his computer "were never physically present in Virginia," the court also noted that "is equally accurate that the warrant did not violate Rule 41(b)(4)'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device used here." *Id.* Ultimately, the court found that "the NIT authorized by the warrant was executed by the FBI from its computer located within the Eastern District of Virginia" and that "*but for* [the defendant] electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed." *Id.* Thus, the court held that "the only

reasonable interpretation of where the information-tracking NIT was 'install[ed]' for purposes of Rule 41(b)(4), is the Eastern District of Virginia, where the tracking device—in this case a string of computer code—was caused to be executed and deployed." *Id.* Thus, the court found that the NIT Warrant was properly issued pursuant to Rule 41(b)(4). *Id.*

Conversely, this Court determined in *Adams* that the NIT Warrant violated Rule 41(b)(4). 2016 WL 4212079, at *6. Specifically, the Court noted that Rule 41(b)(4) allows magistrate judges "to issue a warrant to install within the district a tracking device." *Id.* The Court reasoned, however, that "[b]ecause a tracking device monitors the movement of a person or object, the person or object must be located within the district at the time the tracking device is installed." *Id.* The Court stated that the NIT Warrant only "authorizes the installation of the NIT onto the government-controlled Playpen server and not onto Defendant's computer," which was located outside of the Eastern District of Virginia in Florida. *Id.* The Court did not find persuasive the reasoning of other courts that determined that defendants took a virtual trip to the Eastern District of Virginia. *Id.* Additionally, the Court determined that NIT searches, rather than "tracks." *Id.* The Court stated that "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." *Id.* As a result, the Court determined that the NIT Warrant violated Rule 41(b)(4). *Id.*

Upon review, as noted above, the factual record and the law in this case are virtually identical to the law and facts in this Court's prior decision in *Hart*. Due to the overwhelming similarities in the present case, the Undersigned finds that the same conclusions reached in *Hart* are applicable here. Specifically, the record of this case supports a finding that the NIT Warrant was properly issued as a tracking warrant pursuant to Fed. R. Crim. P. 41(b)(4).

In reaching this conclusion, the Undersigned first finds that the NIT is a "tracking device" under the definition in Rule 41. On this point, the Court finds the reasoning from *Jean* to be especially persuasive. 207 F. Supp. 3d at 942. In *Jean*, the court found that the NIT was a "tracking device." 207 F. Supp. 3d at 942. Here, Agent Alfin's testimony supports the same conclusion. Specifically, Agent Alfin testified at the hearing that the NIT was computer code that resided on a Government server in the Eastern District of Virginia where the Government was running the Playpen website. (Tr. at 30). Agent Alfin further indicated that the NIT traveled over the Internet. (*Id.*). Thus, as in *Jean*, the record supports a finding that the NIT is an "electronic device" as that term is defined in 18 U.S.C. § 3117(b) because the NIT is "an investigative tool consisting of computer code transmitted electronically over the internet." *See Jean*, 207 F. Supp. 3d at 942.

Similarly, Agent Alfin's testimony supports the conclusion that the purpose of the NIT was to track the movement of property. *See id.* Specifically, Agent Alfin testified that when users requested information from the Playpen website, the NIT code was attached to that information and traveled to that user's computer. (*Id.* at 30:18-19). That code then forced the activating computer to send to the Government "the real IP address of the computer, along with a minimal amount of other identifying information." (*Id.* at 30:19-22). Agent Alfin testified that all of the information sought by the NIT was aimed at determining the final location of the NIT. (*Id.* at 34:22-23). Agent Alfin testified that the IP address was the most valuable piece of information because it can be used to identify a physical address. (*Id.* at 35-36). Agent Alfin testified that the rest of the information sought by the NIT was designed to determine the specific device and user among the various potential devices and users that may be associated with a particular IP address. (*Id.* at 35). Stated differently, the NIT attached itself to information on the

Playpen server in Virginia that Defendant voluntarily requested be sent to his computer in Florida. The NIT tracked that information back to Defendant's local computer, reporting its final location in the form of an IP address and other narrowly tailored information that pinpointed the specific device and user accessing the Playpen website. Thus, the record supports a finding that the purpose of the NIT was to track "property"—*i.e.*, intangible information. *See Jean*, 207 F. Supp. 3d at 942.

Accordingly, as in *Jean*, the record supports a finding that NIT is a tracking device because (1) it is an "electronic device" within the meaning of 18 U.S.C. § 3117(b) and (2) its purpose was to track the movement of property. *See id.* Thus, the Undersigned finds that the NIT qualifies as a "tracking device" pursuant to the Rule 41(a)(2)(A).

Having found that the NIT qualifies as a tracking device, the Undersigned now addresses whether the NIT was installed in the district where the warrant was issued—*i.e.*, the Eastern District of Virginia. On this point, the Undersigned finds the opinions in *Hart*, *Darby*, and *Jean* to be highly persuasive.

In *Hart, Darby*, and *Jean*, the courts likened the defendant's actions to taking a "virtual trip." In *Hart*, this Court found that the defendant virtually visited the Eastern District of Virginia because but for defendant's voluntary actions, the NIT would have remained dormant in the Eastern District of Virginia and never deployed in the defendant's computer in Florida. No. 2:16-CR-110-FTM-29CM, slip op. Doc. 50 at 19. Similarly, the court in *Darby* found that Playpen users "digitally touched down in the Eastern District of Virginia when they logged into the site." 190 F. Supp. 3d at 536. Further, the court in *Jean* found that "*but for* [the defendant] electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed." 207 F. Supp. 3d at 943.

The Undersigned finds the analogy of a "virtual trip" to be highly persuasive and apt. Although any analogy drawn from the physical world is likely under these circumstances to be imperfect on some level when used to conceptualize events occurring in a digital realm, it is clear from the record that Defendant's conduct in the Middle District of Florida caused the Playpen server in the Eastern District of Virginia to transmit information (to which the NIT was attached) to his local computer. The NIT was installed in the first instance on the server in Virginia and would not have traveled – like sidewalk gum stuck to the bottom of an unwitting traveler's shoe – to Defendant's computer in Florida but for Defendant's virtual presence in the Eastern District of Virginia. (Tr. at 30-31).

Additionally, while it is true that the NIT completed its operation in Florida, the Undersigned finds that this does not change the analysis. Specifically, similar to this Court's decision in *Hart*, No. 2:16-CR-110-FTM-29CM, slip op. Doc. 50 at 20, the record here also shows that the NIT operated quickly—usually in less than one second. (Tr. at 31-32). As in *Hart*, Agent Alfin testified here that nothing was installed on an end user's computer and that nothing remained on the user's computer after the NIT finished its operation. (*Id.* at 32, 37). Additionally, the FBI had no ability to access the computer again after the NIT performed its operation. (*Id.* at 39). Thus, despite the fact that the NIT's operation occurred in Florida, as the court in *Jean* aptly stated, "the only reasonable interpretation of where the information-tracking NIT was 'install[ed]' for purposes of Rule 41(b)(4), is the Eastern District of Virginia" because that is where the tracking device – *i.e.*, the NIT's computer code – "was caused to be executed and deployed." 207 F. Supp. 3d at 943. Accordingly, the Undersigned finds that the tracking device was installed in the Eastern District of Virginia.

The question then becomes whether the NIT "tracked" or whether it did something else, such as perform a search. Courts have reached divergent conclusions on this issue. In *Adams*, for instance, this Court determined that Rule 41(b)(4) was violated because the Court determined that NIT searches rather than tracks. 2016 WL 4212079, at *6. In *Hart*, however, this Court found that the NIT tracked rather than searched. *Hart*, No. 2:16-cr-110-FTM-29CM, slip op. Doc. 50 at 21. Here, based on the overwhelming similarities in the records of the two cases, the Undersigned is persuaded by the opinion in *Hart* and finds that the NIT "tracked" rather than "searched" and, therefore, complied with Rule 41(b)(4).

Upon review, the NIT Warrant and the NIT did not exceed what was allowed by Rule 41(b)(4). As a result, the Undersigned finds that the NIT Warrant was authorized by Rule 41(b)(4) and did not violate the Rule. Furthermore, because a magistrate judge's authority to issue warrants is derived from the Federal Rules of Criminal Procedure, the Undersigned finds that the NIT Warrant did not violate the Federal Magistrates Act. *See Taylor*, 2017 WL 1437511, at *12. Stated differently, the record supports a finding that Magistrate Judge Buchanan fully complied with the Federal Rules of Criminal Procedure. As such, the NIT Warrant was validly issued, and there was no violation of the Federal Magistrates Act. Accordingly, Defendant's Motion to Suppress should be denied on this ground.

3. Alternative Arguments

Although the Undersigned finds that the NIT Warrant was validly issued, the Undersigned will nevertheless address Defendant's alternative arguments. Specifically, Defendant argues that the evidence obtained from the NIT Warrant should be suppressed because (1) a violation of Rule 41(b) renders the NIT Warrant void *ab initio* and, thus, makes the Government's actions the equivalent of a warrantless search and/or (2) the NIT Warrant's

violation of Rule 41(b) was prejudicial to Defendant. (Doc. 17 at 15-18). Upon review, however, even assuming *arguendo* that the NIT Warrant violated Rule 41(b), suppression would not be warranted.

Specifically, the Supreme Court has indicated that the exclusion (suppression) of evidence is a "last resort" not a "first impulse." *Herring v. United States*, 555 U.S. 135, 140 (2009). The exclusionary rule is not an individual right and applies only where it results in appreciable deterrence. *Id.* (quotation marks omitted; citing *United States v. Leon*, 468 U.S. 897, 909 (1984)). The exclusionary rule only applies where it serves to deter *future Fourth Amendment violations*. *Id.* Moreover, "the benefits of deterrence must outweigh the costs." *Id.* (citing *Leon*, 468 U.S. at 910). The Supreme Court has rejected the suggestion that the exclusionary rule should apply where there would be only marginal deterrence. *See id.*

On this point, the Undersigned has found that the NIT Warrant sufficiently complied with the general requirements of the Fourth Amendment. *See King*, 563 U.S. at 459; *Dalia*, 441 U.S. at 255. Without a violation of the Fourth Amendment, it is unclear what future Fourth Amendment violations could be deterred. Notwithstanding this finding, the Undersigned notes that Defendant posed an additional argument that the NIT Warrant's issuance in violation of Rule 41(b) renders it void *ab initio*. (Doc. 17 at 16). Defendant contends that this renders the actions of the Government the equivalent of a warrantless search. (*Id.*).

This argument appears to have originated from the concurring opinion of former Circuit Judge Neil Gorsuch in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015). In *Krueger*, the Tenth Circuit affirmed the district court's decision to suppress the defendant's statements when a warrant was issued in Kansas but executed in Oklahoma. *Id.* at 1117. There, the court determined that Rule 41(b) was violated and found that the defendant had demonstrated

sufficient prejudice to warrant suppression of the evidence. *Id.* In his concurring opinion, however, Judge Gorsuch noted that the court had not reached the issue of whether a warrant issued in violation of Rule 41 remains a warrant for purposes of the Fourth Amendment. *Id.* at 1126. In his opinion, Judge Gorsuch wrote that a warrant issued in violation of Rule 41(b) "is no warrant at all" for purposes of the Fourth Amendment. *Id.* at 1126.

Some courts have adopted this reasoning and ultimately suppressed evidence. *Levin*, 186 F. Supp. 3d at 41-42. Nevertheless, other courts, including this Court, have declined to follow this reasoning, noting that it is based, in part, on a separate Sixth Circuit opinion, *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001), that was effectively overruled in *United States v. Master*, 614 F.3d 236 (6th Cir. 2010). *Kneitel*, 8:16-cr-0023-MSS-JSS, slip op. at Doc. 158 at 2. Additionally, the Undersigned notes that this Court previously found that a violation of Rule 41(b) by the NIT Warrant did not render it void *ab initio*. *Adams*, 2016 WL 4212079, at *6. In *Adams*, this Court held that because Magistrate Judge Buchanan had the inherent power to issue search warrants, any violation of Rule 41(b) by the NIT Warrant was only a technical or procedural violation and not a violation of the Fourth Amendment. *Id.*

Upon review, even assuming *arguendo* that the NIT Warrant was invalid pursuant to Rule 41(b), the Undersigned declines to find that the NIT Warrant was void *ab initio* such that it was "no warrant at all" for purposes of the Fourth Amendment. Instead, the Undersigned agrees with the reasoning in *Adams* that because Judge Buchanan had the inherent power to issue warrants, any potential violation of Rule 41(b)(4) by the NIT Warrant is not a constitutional violation but, at most, a procedural or technical violation. *See id.*

In the absence of a constitutional violation, the Eleventh Circuit has indicated that there are only two instances warranting suppression for violations of Rule 41. *United States v. Loyd*,

721 F.2d 331, 333 (11th Cir. 1983). Specifically, unless there is a clear constitutional violation, the court has stated:

> Rule 41 requires suppression of evidence only where (1) there was "prejudice" in the sense that the search might 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.

Id. (quoting *United States v. Stefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981)).

In *Adams*, this Court found that the defendant had "clearly proven that he was prejudiced by the violation of Rule 41(b)" in connection with the NIT Warrant. 2016 WL 4212079, at *8. The Court stated that "[t]he application in support of the NIT warrant makes it abundantly clear that law enforcement had no realistic chance of identifying the IP address associated with Defendant's computer without the NIT." *Id.* The Court stated that "[h]ad the magistrate judge followed Rule 41(b), the search of Defendant's computer would not have occurred." *Id.* Thus, the defendant was prejudiced by the violation of Rule 41(b). *Id.*

Assuming, *arguendo*, that there was a violation of Fed. R. Crim. P. 41(b), Defendant has adequately shown that he was prejudiced by the violation of the Rule. Specifically, it is abundantly clear that law enforcement had no realistic chance of identifying Defendant's IP address without the NIT due to the nature of the Tor network. *See Adams*, 2016 WL 4212079, at *8. The NIT was authorized by the NIT Warrant. If Rule 41(b) had been followed, then the NIT Warrant would not have been issued, and the search of Defendant's residence would not have occurred. *See id.*

Notwithstanding Defendant's ability to show prejudice, the Supreme Court has recognized a so-called "good-faith exception" for warrants. *See Leon*, 468 U.S. at 922. Specifically, the Supreme Court has indicated that the exclusionary rule should not be applied to bar the use in the prosecution's case in chief of evidence obtained by officers acting in

reasonable reliance on a search warrant issued by a detached and neutral magistrate but that is ultimately found to be invalid. *Id.* at 921. The Court stated that "[i]n the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient." *Id.* The Court noted that once a warrant has been issued, "there is literally nothing more the policeman can do in seeking to comply with the law." *Id.* (citing *Stone v. Powell*, 428 U.S. 465, 497 (1976)). The Court stated that "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.*

The Supreme Court has articulated four circumstances in which the good-faith exception does not apply. *See id.* at 922-23. Specifically, the Court stated the exception does not apply when (1) "the magistrate or judge in 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," (2) "the issuing magistrate wholly abandoned his judicial role," (3) the affidavit supporting an application for a warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," and (4) "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* at 923.

In *Adams*, even though the defendant had shown that he was prejudiced by a violation of Rule 41, this Court nevertheless found that the good-faith exception applied. 2016 WL 4212079, at *8. Specifically, this Court found that the FBI agents "acted upon the NIT warrant with objectively reasonable reliance on the warrant's authority." *Id.* (citing *Leon*, 468 U.S. at 922). The Court found that the defendant "failed to offer evidence that the agents possessed some

unique knowledge rendering their reliance upon the NIT warrant objectively [un]reasonable." *Id.*

Similarly, in *Kneitel*, this Court again found that even though the NIT Warrant was issued in violation of Rule 41(b), the good-faith exception applied. 8:16-cr-0023-MSS-JSS, slip op. at Doc. 158 at 2, 6. The Court indicated that no Eleventh Circuit authority existed suggesting that the good-faith exception could not apply under the circumstances presented by the NIT Warrant. *Id.* at 2.

Here, Defendant argues that the good-faith exception does not apply. (*Id.* at 19-21). Defendant contends that federal agents could not have had a good-faith belief that the NIT Warrant was in compliance with Rule 41(b). (*Id.* at 20). Defendant argues that Agent Macfarlane "was a veteran agent who would have known the then-existing warrant jurisdictional limitations of Rule 41(b) and also known how the NIT worked." (*Id.*). Additionally, at the hearing, Defendant argued that the Government's actions showed bad faith because they misled Judge Buchanan into thinking that she was signing a warrant only for her jurisdiction. (Tr. at 114). Further, Defendant contends that federal agents should have been aware of a proposed amendment to Rule 41(b) that would have allowed the NIT. (Doc. 17 at 20).[9]

The Government argues that the good-faith exception applies because the FBI acted in good faith. (*Id.* at 26). The Government contends that Defendant cannot show that any of the four circumstances that prevent the application of the good-faith exception apply here. (*Id.*).

[9] Defendant also argues that the good-faith exception does not apply because the NIT Warrant fails to meet the particularity requirements of the Fourth Amendment and because the NIT Warrant was void *ab initio*. (Doc. 17 at 21). The Undersigned, however, has specifically made contrary findings above and, therefore, declines to address those arguments again here.

Additionally, the Government points out that the vast majority of courts have determined that the good-faith exception applied to the NIT Warrant. (*Id.* at 29).

Upon review, the facts of this case demonstrate that the good-faith exception applies such that suppression is not warranted even assuming, *arguendo*, that the NIT Warrant violated Rule 41(b). Specifically, the good-faith exception applies when officers act in reasonable reliance on a search warrant issued by a detached and neutral magistrate judge. *See Leon*, 468 U.S. at 921. Here, there is no indication in the record that the FBI agents failed to act in reasonable reliance on a search warrant issued by a detached and neutral magistrate judge. *See id*.

Specifically, although Defendant argues that federal agents should have known the jurisdictional limitations of Rule 41(b), there is no evidence of record demonstrating that the FBI agents acting on the NIT Warrant knew or should have known that the NIT Warrant violated Rule 41(b). Agent Alfin testified that he had no reason to believe the NIT Warrant was invalid. (Tr. at 40). Agent Alfin testified that he worked closely with DOJ attorneys, lawyers in the FBI Office of General Counsel, and other FBI agents who all reviewed the NIT Warrant in coming to that conclusion. (*Id.*). Moreover, the Undersigned finds the fact that courts around the country reached differing conclusions demonstrates that reasonable minds can differ as to the legality of the NIT Warrant's compliance with Rule 41(b). The issue certainly was not settled at that time such that any FBI agent reviewing the NIT Warrant would have known with certainty that the NIT Warrant was invalid. Notwithstanding any uncertainty, the FBI affirmatively sought and obtained a warrant from a neutral and detached magistrate judge as they would normally be required to do. Once the FBI obtained a warrant, there was literally nothing else they could do to comply with the law beyond compliance with the bounds of the warrant itself. *See Leon*, 468

U.S. at 923. As such, it would make little sense to penalize the FBI for any error by the magistrate judge.

Similarly, although Defendant contends that federal agents should have been aware of a proposed amendment to Rule 41(b) that would have allowed the NIT, (Doc. 17 at 20), there is no evidence of record to support a finding that the FBI agents who executed the NIT Warrant had any knowledge of the proposed amendment to Rule 41(b) such that their actions related to the NIT Warrant may be considered bad faith.

Furthermore, the Supreme Court has noted four circumstances in which the good-faith exception does not apply. *See Leon*, 468 U.S. at 923. None of those circumstances are present in this case.

First, there is no indication that Judge Buchanan was misled by information in Agent Macfarlane's Affidavit in support of the NIT Warrant or that Agent Macfarlane knew the information in the Affidavit was false or would have known the information was false except for his reckless disregard of the truth. *See id.* Defendant makes no argument that information set forth in Agent Macfarlane's Affidavit was false.

Second, there is no indication that the issuing magistrate judge wholly abandoned her judicial role. *See Leon*, 468 U.S. at 923. Defendant makes no argument that the NIT Warrant was issued by a magistrate judge who failed to be neutral and detached, and the record does not otherwise support a finding that the magistrate judge failed to dutifully perform her judicial role.

Third, Defendant did not argue that the NIT Warrant lacked probable cause. As such, the circumstance in which an affidavit supporting an application for a warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" is not present in this case. *See Leon*, 468 U.S. at 923.

Finally, the NIT Warrant is not facially deficient. *See id.* As the Undersigned discussed above, the NIT Warrant states with particularity the place to be searched and the items to be seized. (*See* Discussion *supra* at Part II.A.1.). Thus, there is no indication that the executing officers should have presumed the NIT Warrant was invalid on its face. *See Leon*, 468 U.S. at 923.

As a final consideration, exclusion is only warranted where it serves to deter future Fourth Amendment violations. *Herring*, 555 U.S. at 140. Even assuming, *arguendo*, that a Fourth Amendment violation of some sort occurred, it is unclear what future violations could be deterred by the exclusion of the evidence in this case. Along these lines, as the parties have noted, Federal Rule of Criminal Procedure 41(b) has since been amended. The present version of the Rule added the following provision:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Fed. R. Crim. P. 41(b)(6) (2016). Under Fed. R. Crim. P. 41(b)(6), as amended, it appears that techniques such as the NIT are now expressly contemplated by Rule 41(b)(6). As such, it makes little sense to suppress any evidence here when the conduct at issue would now be expressly permitted by the Rule.

Moreover, in weighing the potential benefits and costs of suppression, the Undersigned finds that the costs of suppression far outweigh any potential deterrent effect. On the one hand,

there appears to be little, if any, deterrent effect to suppressing the evidence here. On the other hand, suppression would allow a defendant to evade prosecution for alleged activity that relied on the sexual exploitation of children. Suppression is not warranted in such a situation. *See Herring*, 555 U.S. at 140.

Thus, assuming *arguendo* that the NIT Warrant violated Rule 41(b), the Undersigned nevertheless finds that the good-faith exception applies to the NIT Warrant. Because the exception applies, suppression of evidence would not be warranted even with a violation of the Rule. Accordingly, even if there was a violation of Rule 41(b), the Undersigned would still recommend that Defendant's Motion to Suppress Evidence (Doc. 17) be denied on this ground.

B. Naples Search Warrant

Defendant's second request for suppression is based on an argument that the Naples Search Warrant at his residence was tainted by the illegal search of Defendant's computer through the NIT. (Doc. 17 at 18). Defendant argues that "probable cause did not exist, for the Naples Warrant, absent the illegally obtained information from the NIT search of the Defendant's computer." (*Id.* at 19).

Here, the Undersigned notes that Defendant does not dispute that probable cause existed for the Naples Search Warrant in light of the results of the NIT Warrant. Instead, Defendant only argues that there is no probable cause without the information obtained through the tainted NIT Warrant. For the reasons set forth extensively above, however, the Undersigned finds that the information obtained from the NIT Warrant was not obtained illegally. Because the information in support of the Naples Search Warrant was not obtained illegally, Defendant's argument as to the Naples Search Warrant fails. The Undersigned, therefore, recommends that Defendant's Motion (Doc. 17) be denied on this ground.

C. Defendant's Statements

Defendant's final contention is that all statements to federal agents should be suppressed because he was subjected to a custodial interrogation without the benefit of *Miranda* warnings. (Doc. 17 at 21). In response, the Government does not contest that an interrogation occurred. (Doc. 22 at 31-33). Instead, the Government argues that the statements should not be suppressed because Defendant was not "in custody" and, thus, not entitled to *Miranda* warnings. (*Id.*).

Miranda v. Arizona stands for the proposition that when "an individual is taken into custody or otherwise deprived of his freedom by the authorities in any significant way and is subjected to questioning, the privilege against self-incrimination is jeopardized." 384 U.S. 436, 478 (1966). A person subject to a custodial interrogation is entitled to certain warnings. *See id.* The warnings include being informed of the right to remain silent and that anything said can be used against a person in a court of law. *Id.* at 479. Additionally, a person must be told that he or she has the right to the presence of an attorney, and that if he or she cannot afford an attorney one will be appointed for him or her prior to any questioning. *Id.*

A defendant has the right to *Miranda* warnings when a custodial interrogation begins. *United States v. Brown*, 441 F.3d 1330, 1347 (11th Cir. 2006) (citing *United States v. Acosta*, 363 F.3d 1141, 1148 (11th Cir. 2004)). "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.'" *Id.* (citing *California v. Beheler*, 463 U.S. 1121, 1125 (1983)).

The "initial step" in determining whether someone is in custody is to determine whether – in light of the objective circumstances of the interrogation – a reasonable person would have felt he or she was not at liberty to terminate the interrogation and leave. *Howes v. Fields*, 565 U.S. 499, 509 (2012) (internal citations and quotation marks omitted); *see also United States v.*

Maldonado, 562 F. App'x 859, 860 (11th Cir. 2014). This test is objective. *Brown*, 441 F.3d at 1347. The actual, subjective beliefs of a defendant and the interviewing officer on the question of whether the defendant was free to leave are irrelevant. *Id.* (citing *United States v. Moya*, 74 F.3d 1117, 1119 (11th Cir. 1996)). Instead, the Eleventh Circuit has stated that "under the objective standard, the reasonable person from whose perspective 'custody' is defined is a reasonable innocent person." *Moya*, 74 F.3d at 1119.

The Court evaluates many relevant factors to determine if a person was "in custody." Relevant factors include the location of the questioning, the duration of questioning, statements made during the interview, the presence or absence of physical restraints during the questioning, and the release of the interviewee at the end of the questioning. *Howes*, 565 U.S. at 509; *see also United States v. Matcovich*, 522 F. App'x 850, 851 (11th Cir. 2013). Other factors include whether officers brandished weapons, touched the suspect, or used language or a tone indicating that compliance with the officers could be compelled. *United States v. Street*, 472 F.3d 1298, 1309 (11th Cir. 2006) (citations omitted).

In reviewing relevant factors, the Undersigned first notes that the location of the interview occurred in Defendant's home. (Tr. at 70). Although not dispositive, "[c]ourts are *much less likely* to find the circumstances custodial when the interrogation occurs in familiar or at least neutral surroundings, such as the suspect's home." *Brown*, 441 F.3d at 1348 (original emphasis; citations and quotation omitted). Here, because the interrogation occurred in the familiar surroundings of his home, the Undersigned finds that the location of the interview weighs against Defendant's contention that the interrogation was custodial. *See id.*

Another important factor courts consider is whether a defendant was unambiguously advised that he or she is free to leave and is not in custody. *Id.* at 1347. The Eleventh Circuit

has stated that advising a defendant that he or she is free to leave and not in custody "is a powerful factor in the mix, and generally will lead to the conclusion that the defendant is *not* in custody absent a finding of restraints that are so extensive that telling the suspect he was free to leave could not cure the custodial aspect of the interview." *Id.* (citations and quotation marks omitted). Further, a defendant's statement that he understood the officers' advice that he or she was not under arrest and was free to leave strengthens the force of the instructions. *Id.* at 1348.

On this point, the record shows that Officer Bunch unambiguously advised that he was free to leave and not under arrest. (Gov. Ex. 3t, Doc. 29-5 at 4). After this advice, Defendant stated on multiple occasions that he understood. (*Id.*). Because Defendant was advised that he was free to leave with his children and was not in custody, and because Defendant stated that he understood those facts, the Undersigned finds these factors weigh heavily against Defendant's contention that he was in custody. *See Brown*, 441 F.3d at 1347.

Furthermore, while Defendant was not allowed to enter his house due to safety reasons, Defendant was not physically restrained during the interrogation. (Tr. at 74). Similarly, while weapons were drawn when the agents entered Defendant's house (Tr. at 78), those weapons were not brandished during the interview (Tr. at 70). Upon review, there is no indication that any restraints on Defendant's movement were so extensive that telling Defendant that he was free to leave could not cure any custodial aspect of the interview. *See Brown*, 441 F.3d at 1347. Thus, the Undersigned concludes that these factors weigh against Defendant.

Finally, the Undersigned notes that Defendant was released at the end of the questioning. Defendant's release at the end of questioning weighs against Defendant's contention that he was in custody for the interview. *See Howes*, 565 U.S. at 509.

In sum, a review of the relevant factors demonstrates that Defendant was not in custody. Because Defendant was not in custody, Defendant was not entitled to *Miranda* warnings. Accordingly, Defendant's statements to law enforcement should not be suppressed because his rights were not violated. The Undersigned, therefore, recommends that Defendant's Motion to Suppress Evidence (Doc. 17) be denied on this ground.

III. Conclusion

Based on the foregoing, Defendant's Motion is due to be denied in its entirety. Accordingly, the Undersigned hereby **RESPECTFULLY RECOMMENDS**:

That Defendant's Motion to Suppress Evidence (Doc. 17) be **DENIED**.

Respectfully recommended in Chambers in Fort Myers, Florida on July 11, 2017.

MAC R. MCCOY
UNITED STATES MAGISTRATE JUDGE

NOTICE TO PARTIES

A party has fourteen days from this date to file written objections to the Report and Recommendation's factual findings and legal conclusions. A party's failure to file written objections waives that party's right to challenge on appeal any unobjected-to factual finding or legal conclusion the district judge adopts from the Report and Recommendation. *See* 11th Cir. R. 3-1.

Copies furnished to:

Counsel of Record
Unrepresented Parties