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

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND STATEMENTS

COMES NOW the United States of America by W. Steven Muldrow, Acting United States Attorney for the Middle District of Florida, and hereby responds to the defendant's motion to suppress (doc. 17). The defendant seeks to suppress evidence that the United States obtained pursuant to two search warrants – one in the Eastern District of Virginia and the other from the Middle District of Florida. The defendant does not argue that the warrants lacked probable cause, but instead, that the computer code that the warrant authorized, which tracked the movement of child pornography to the defendant's computer when the defendant downloaded it, violated his expectation of privacy. The defendant also seeks to suppress his August 6, 2015 statement to FBI agents, which he made during a consensual non-custodial interview on his own back lanai after FBI agents informed him that he did not need to speak to them and was free to leave. The Court should

deny the defendant's motion.

BACKGROUND

The charges against the defendant in this case stem from an investigation into Playpen, a global online forum dedicated to the advertisement and distribution of child pornography through which registered users, including the defendant, accessed and viewed illegal child pornography. *See NIT Search Warrant, Application and Affidavit*, Attachment 1 (hereinafter "the NIT warrant").[1] Various courts around the country have already decided the defendant's first two arguments at least 49 times, and other decisions are currently pending.

I. THE TOR NETWORK, THE PLAYPEN WEBSITE AND THE EFFORTS TO AVOID DETECTION

Playpen operated as a "hidden service" on the anonymous Tor network, which has both legitimate and illegal uses, such as making child pornography available to users. *Id.* ¶ 7. The Tor network masks the user's actual IP address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes"). *Id.* ¶ 8. To access the Tor network, users must install Tor software. *Id.* ¶ 7. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address. *Id.* ¶ 8.

[1] At the time of the search warrant, the investigation was then ongoing so Playpen was referred to as "Website A."

The Tor is designed to prevent tracing the user's actual IP address. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable with the Tor network. *Id.*

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." *Id.* at ¶ 9. Like other websites, they are hosted on computer servers that communicate using IP addresses. *Id.* They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix "onion." *Id.* A user can only reach a "hidden service" by using the Tor client and operating in the Tor network.

A "hidden service," like Playpen, is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" to access it. *Id.* at ¶ 10. To find Playpen, a user had to first obtain its web address from another source - such as another Playpen user or online postings identifying Playpen's content and location. It is highly unlikely that any user stumbled upon it without first understanding its child pornography-related content and purpose. *Id.*

FBI agents apprehended the administrator of Playpen in the Middle District of Florida and seized the website from its web-hosting facility in

North Carolina in February 2015. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified and un-apprehended, the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia for the brief period from February 20, 2015 through March 4, 2015.

II. THE NIT SEARCH WARRANT

A veteran FBI agent with over 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children swore to the 31-page NIT search warrant affidavit. *Id.* at ¶ 1. In his motion, Caswell does not dispute that the NIT search warrant affidavit established probable cause.

The agent also described the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." *Id.* In addition, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." *Id.* The agent also explained the massive scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen – which was believed to have been in existence only since August 2014 – showed that it

contained 158,094 members, 9,333 message threads, and 95,148 posted messages. *Id*. at ¶ 11. Images and videos shared through the site were highly categorized according to victim age range and gender, and the type of sexual activity portrayed. *Id*. at ¶ 14. The site also included forums for discussion of all things related to child sexual exploitation, including tips for grooming victims and avoiding detection. *Id*. at ¶ 16-20

As described in the affidavit, Playpen's illicit purpose was apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." *Id*. at ¶ 12. The following text appeared beneath those young girls: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being "re-posted" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." *Id*.

As set forth in the affidavit, users were required to register an account by creating a username and password before they could access the site and to review and accept the registration terms, which placed an emphasis on user

anonymity. *Id*. at ¶¶ 12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, including encouraging fake e-mail addresses and change their computer settings and notifying users "[t]his website is not able to see your IP." *Id*. at ¶ 13. Child pornography files were posted and available to all registered users of Playpen, including images showing adults sexually abusing prepubescent children and even toddlers. *Id*. at ¶ 18. "[T]he entirety of [Playpen was] dedicated to child pornography," and a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id*. at ¶ 27.

In the NIT search warrant affidavit, the FBI agent provided a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, and what information it would collect. Specifically, the agent noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." *Id.* at ¶ 29. Further, because of the "unique nature of the Tor network and the method by which the network … route[s] communications through multiple other computers … other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or

reasonably appear to be unlikely to succeed." The affiant thus concluded, "using a NIT may help FBI agents locate the administrators and users" of Playpen. *Id.* at ¶¶ 31-32. Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove … the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. *Id.* at ¶ 31.

The NIT was installed in the Eastern District of Virginia. *Id.* at ¶ 32. The NIT consisted of additional computer instructions. When a user logged onto the website maintained in the Eastern District of Virginia, the NIT computer instructions would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal access to and operation of the website. *Id.* at ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. *Id.* The agent listed the pieces of information to be collected in the warrant and accompanying Attachment B, along with technical explanations of the terms:

(1) the actual IP address assigned to the user's computer;

(2) a unique identifier assigned by the FBI to distinguish the data

from that of other computers;

(3) the operating system running on the computer;

(4) information about whether the NIT had already been delivered to the computer;

(5) the computer's Host Name;

(6) the computer's active operating system username; and

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

Id. at ¶ 34.

All of those items were either generated by the FBI (items 2 and 4), or related to the location of the computer:

> the actual IP address of a computer that accesses [Playpen] can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

Id.

Finally, the NIT warrant contemplated that the NIT would travel outside the Eastern District of Virginia. Specifically, the Court authorized the NIT to "cause an activating computer – wherever located – to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other

information about the computer and the user of the computer." *Id.* at ¶ 46(a).

III. THE RESIDENTIAL SEARCH WARRANT AFFIDAVIT, AND THE DEFENDANT'S NON-CUSTODIAL INTERVIEW.

Using the NIT, law enforcement agents identified an IP address associated with the Playpen user "*whaddupyall*" after the defendant accessed a site that appeared to contain child pornography. *See Caswell's Residence Search Warrant Affidavit,* Attachment 2, ¶¶ 33-37 (hereinafter "the residential search warrant"). Agents then captured the activity of the user "whaddupyall" on the Playpen website. That user logged 15 hours of activity on the Playpen website between the dates of January 26, 2015 and March 4, 2015. *Id*. at ¶ 32. During that time, the user accessed posts that contained links to child pornography. *Id*. at ¶¶ 36, 37. Through independent investigation, the agents determined defendant's physical address located in the Middle District of Florida. *Id.* at ¶ 41. On July 27, 2015, United States Magistrate Judge Mac R. McCoy issued a federal search warrant authorizing the search of Caswell's residence for evidence of child pornography. *Id*.

Law enforcement officers executed the search warrant at the defendant's residence on August 6, 2015. Caswell was present at the residence and agreed to a non-custodial interview while other agents were inside conducting the search. The two interviewing agents recorded the interview on an audio recording device, and the interview was later

transcribed. The agents did not have their guns drawn during the interview, nor did they use physical restraints. The interview occurred on the defendant's back lanai.

Agents repeatedly told the defendant he did not need to speak to them and that he was free to leave. Specifically, one of the interviewing agents informed Caswell that they were executing a search warrant, and that he was "not under arrest." The agent continued "[y]ou could leave at any time. And any time, you can stop talkin' to - - you can say, 'Bunch, Zac, I'm done talkin' to you." The defendant replied "I watch the shows." The agent continued to say that Caswell could "walk away." The agents cautioned that "we're doin' a search warrant" so "we gotta limit where you go in the house," but "if you wanna walk out your lanai, hop the fence and go, I'll wave [sic] to ya." The agent continued that "if you have to get up, let me know. Or if you wanna leave, let me know." Throughout the course of the interview, agents reminded the defendant that they were not going to take him to jail after the interview, and that the agents were "leaving here today. You're staying here." During the interview, the defendant admitted to, among other things, accessing the Playpen website and viewing child pornography. In a subsequent conversation with one of the interviewing FBI agents, the defendant admitted to creating and using the username "whaddupyall." The FBI seized the defendant's computer and located images and videos of child

pornography in a desktop folder.

MEMORANDUM OF LAW

The defendant has moved to suppress evidence on three grounds, advancing essentially two arguments. First, the defendant argues that, although supported by probable cause, the United States Magistrate Judge in the Eastern District of Virginia lacked the authority under Rule 41(b) to issue the NIT warrant and, consequently, the residential search warrant was the fruit of an illegal prior search. Second, the defendant argues that FBI agents were required to issue the defendant *Miranda* warnings despite the fact that the defendant was not in custody during interview. Each of those arguments is considered in turn.

I. THE MAGISTRATE JUDGE IN THE EASTERN DISTRICT OF VIRGINIA PROPERLY ISSUED THE NIT WARRANT.

A. The NIT was properly authorized as a tracker pursuant to Fed. R. Crim. P. 41(b)(4)

Rule 41(b)(4) of the Federal Rules of Criminal procedure 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." *Id.* Critically, the term "property" applies to both tangible property (i.e. a stolen vehicle), or intangible property (i.e. "information," such as a computer file that contains

child pornography). *See* Fed. R. Crim. P. 41(a)(2) ("'[p]roperty' includes documents, books, papers, any other tangible objects, *and information*.") (emphasis added). In addition, 18 U.S.C. § 3117(b) defines "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *Id*. At least 14 other courts that have considered this issue have held that the NIT is a properly-issued tracker pursuant to Rule 41(b)(4).[2]

When considering whether a NIT is a "tracker," courts have considered at least two sub-issues: (1) whether the NIT is "installed" in the Eastern District of Virginia, or on a given defendant's out-of-district computer; and (2)

---

[2] *United States v. Austin*, No. 3:16-cr-68, 2017 WL 496374 (M.D. Tenn. Feb. 2, 2017); *United States v. Jones*, No. 3:16-cr-26, 2017 WL 511883 (S.D. Ohio Feb. 2, 2017); *United States v. Sullivan*, No. 1:16-cr-270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); *United States v. Bee*, No. 16-002, 2017 WL 424905 (W.D. Mo. Jan. 13, 2017) (magistrate's report and recommendation); *United States v. McLamb*, No. 16-cr-092, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); *United States v. Lough*, No. 16-cr-18, 2016 WL 6834003 (N.D. W.Va. Nov. 18, 2016); *United States v. Kienast*, No. 16-CR-103, 2016 WL 6683481 (E.D. Wisc. Nov. 14, 2016); *United States v. Mascetti*, No. 16-cr-308 (M.D.N.C. Oct. 24, 2016); *United States v. Johnson*, No. 15-cr-00340, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Smith*, No. 15-CR-00467 (S.D. Tx. Sept. 28, 2016); *United States v. Jean*, No. 15-cr-50087, 2016 WL 4771096 (W.D. Ark. Sep. 13, 2016); *United States v. Eure*, No. 2:16-CR-43, 2016 WL 4059663 (E.D. Va. Jul. 28, 2016) (incorporating *Darby*, authored by same judge); *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776, (E.D. Va. June 23, 2016); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016). *See also United States v. Laurita*, No. 8:13CR107, 2016 WL 4179365 (D. Neb. Aug. 5, 2016) (finding similar 2012 NIT warrant deployed on Tor network child pornography website properly authorized under tracking device provision of Rule 41(b)(4)).

whether the NIT "searches" instead of "tracks." Those issues are considered in turn.

1. *The FBI "Installed" the NIT in the Eastern District of Virginia*.

Both Rule 41(b)(4) and the NIT warrant in this case contemplate that a tracking device may leave the jurisdiction in which it is installed. *See* Fed. R. Crim. P. 41(b)(4) (providing that a tracker may "track the movement . . . within the district, *outside the district*, or both.") (emphasis added); NIT Warrant at ¶ 46(a) ("the NIT may 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.") (emphasis added).

The FBI installed the NIT code on the Playpen server, which was located in the Eastern District of Virginia. *NIT Warrant* at ¶ 32. The tracking code would have remained in the Eastern District of Virginia, dormant, but for the defendant reaching into the Eastern District of Virginia and taking the NIT, along with child pornography, back with him to the Middle District of Florida. For example, FBI agents did not remotely hack the defendant's computer and install the NIT on it. FBI agents did not physically travel to the defendant's house and download or "install" the NIT

on the defendant's computer. The FBI did not even volitionally send the NIT to the defendant – the defendant triggered an automatic deployment of the NIT when he accessed child pornography on Playpen.

An analogy to a tracker installed in a brick of cocaine is helpful, albeit imperfect. The analogy is imperfect because cocaine is a tangible object but the child pornography in this case was an intangible item. Nevertheless, consider that the FBI had installed a tracker in a brick of cocaine in the Eastern District of Virginia, and the defendant had picked up that brick of cocaine, and the tracking device, in his truck and brought it back to the Middle District of Florida. The fact that the tracker operated or functioned in Florida (i.e. sent location information from Florida to Virginia) does not mean that the tracker was "installed" in Florida. The same applies here – the fact that the NIT tracker functioned in Florida does not mean it was "installed" there. In fact, the evidence at the hearing will show that nothing was "installed" on the defendant's computer at all because the NIT left no trace. In short, the NIT travelled to Florida because the defendant accessed the NIT from Florida – not because the FBI installed it there.

Other courts agree. For example, the Court in *Jean* articulated:

> "[c]iting *Levin* and *Arterbury*, Mr. Jean argues that the NIT here was 'installed' outside of Virginia, because the NIT was downloaded onto [the defendant's] computer in Arkansas. But such an interpretation of the term 'install' sacrifices substance in favor of mere form. . . [T]he term 'install' is problematic,

> primarily because – in a more traditional scenario – the tracking of tangible property under Rule 41(b)(4) requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property – information – something expressly contemplated by Rule 41(a)(2)(A)."

United States v. Jean, 2016 WL 4771096 (W.D. Ark., Sept. 13, 2016).

The *Matish* court similarly noted that when that computer left Virginia – when the user logged out of Playpen – the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location. *Matish,* 2016 WL 3545776 (finding that the magistrate judge had authority under Rule 41(b)(4) to issue warrant to deploy NIT as a "tracking device," because anyone logging in Playpen made a "virtual trip" to Virginia). The district court in *Darby* similarly reasoned:

> Once installed, [a] tracking device may continue to operate even if the object tracked moves outside the district. This is exactly analogous to what the NIT Warrant authorized. Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location. The magistrate judge did not violate Rule 41(b) in issuing the NIT Warrant.

Darby, 2016 WL 3189703 at *12.

Moreover, if the defendant's interpretation of Rule 41(b)(4) is accurate, there would have been no possible way to obtain the tracker warrant anywhere

in the country. *Jean*, 2016 WL 4771096, *17 ("The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect – or evidence of his crime – may be located. . . . When an unknown crime suspect, or unknown evidence of his crime, is located in an unknown district, it would be nonsensical to interpret the Rule . . . to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. The fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia – is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception.") For those reasons, the tracker warrant was "installed" in the Eastern District of Virginia.

2. The NIT is a "Tracker."

Rule 41(b)(4) allows a tracker to be installed to "to track the movement" of information. Simply stated, the NIT is a tracker because it obtained only information related to location of the child pornography. Specifically, the NIT was designed to obtain (1) the actual IP address assigned to the user's computer, (2) a unique identifier assigned by the FBI to distinguish the data from that of other computers, (3) the operating system running on the computer, (4) information about whether the NIT had already been delivered to the computer, (5) the computer's Host Name, (6) the

computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. Items 1, 2, and 4 do not even reside on the defendant's computer.[3] The other items, including the operating system, host name, username, and MAC address all relate directly to where the child pornography went after it left the Eastern District of Virginia.

The analogy to the tracked brick of cocaine is helpful, but again imperfect, because cocaine is a tangible item and computer files are intangible. Nevertheless, consider that the defendant in the above hypothetical, upon returning to Florida with the tracked cocaine brick, parked his truck containing the brick at a large warehouse complex. Also consider that the tracker in this hypothetical, instead of simply indicating that the brick was at 1234 Metro Parkway, Fort Myers, Florida, indicated more specific location information like warehouse B, garage 5, northeast corner, front right passenger seat. In sum, the NIT here did just that.[4] Not only did the NIT track the

[3] Item 1, the defendant's IP address, resided on the defendant's modem or router. The NIT acquired the defendant's IP address when it caused the defendant's computer to send information back to the Eastern District of Virginia over the "regular" internet, as opposed to over the TOR or "darkweb." The FBI generated items 2 and 4.

[4] The Court in *United States v. Adams*, 6:16-cr-00011-PGB-GJK, doc. 59 (M.D. Fla. Aug. 10, 2016), decided to the contrary and held that "a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage." *Id.* That is true, but if the United States obtains a tracking device pursuant to Rule 41(b)(4), it has the lawful authority to track the location of that stolen car to the defendant's garage, which is what happened, metaphorically, in this case.

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. Critically, just like a standard tracking device, all information that the tracker caused to be sent to the FBI was location information.

As previously cited, at least 14 other courts, so far, have agreed. The *Jean* Court held "the NIT is an 'electronic device' within the meaning of 18 U.S.C. § 3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet." Jean, 2016 WL 4771096 at *16. To be clear, what is significant here is not whether non-public information was transmitted to the FBI – indeed, all tracking devices provide to the government otherwise non-public location information and thus require a warrant. That is precisely why the United States obtained a warrant for the tracker in this case. What is significant here is that the tracker obtained only location-related information.

B. The NIT does not violate the Federal Magistrates Act, 28 U.S.C. § 636.

Contrary to defendant's argument (doc. 24 at 10), the issuance of the NIT warrant complied with the Federal Magistrates Act, 28 U.S.C. § 636. The plain language of § 636(a) vests a United States magistrate judge with

certain powers and duties, including those "conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1).

Under the Federal Magistrates Act, a magistrate judge "shall have" such powers "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law." 28 U.S.C § 636(a). The prepositional phrase beginning "within the district" modifies the verb "shall have," which immediately proceeds that phrase, not the enumerated powers that follow it. Thus, Section 636(a) limits where a magistrate judge may possess such powers, but not necessarily where those powers can have effects. In the warrant context, this means that the warrant must *issue* from a district described in Section 636(a) – for example, the district in which a magistrate judge sits – but not that the warrant's effects must be limited to that district.

The authority on which the defendant relies to support his argument that the issuance of the NIT warrant violated the Federal Magistrates Act, that is, the concurring opinion in *United States v. Krueger*, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring) (doc. 24 at 5), is neither persuasive nor precedential. For the reasons set forth above, this concurrence espouses an incorrect reading of § 636(a). Further, the facts at issue in *Krueger* are distinguishable. In that case, a magistrate judge in Kansas issued a search

warrant for physical property known to be located in Oklahoma. In the case at bar, a magistrate judge issued a warrant allowing the content of a website hosted in the district in which she sat to be augmented with additional computer instructions comprising the NIT, which would be downloaded from the server in that district by users and administrators accessing the site. Magistrate Judge Buchanan's issuance of the NIT warrant complied with the Federal Magistrates Act because she authorized that warrant within the district in which sessions are held by the court that appointed her (and the issuance of such a warrant fell within the powers and duties conferred on her by the Rules of Criminal Procedure for the United States District Court). Accordingly, Judge Buchanan did not act beyond her authority under the Federal Magistrates Act when she authorized the NIT warrant.

C. Suppression is not an appropriate remedy here, and is unwarranted for several reasons

Suppression is a "last resort, not our first impulse," and any benefit to suppressing evidence (general deterrence of law enforcement misconduct) must outweigh the substantial social cost that results when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140-41 (2009). Exclusion is not a personal right conferred by the Constitution and was not "designed to 'redress the injury' occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236 (2011)

(quoting *Stone v. Powell*, 428 U.S. 465, 486 (1976)). Rather, the exclusionary rule is "a judicially created means of effectuating the rights secured by the Fourth Amendment." Accordingly, defendants who seek suppression must clear a "high obstacle," *Herring*, 555 U.S. at 141, and "when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should largely be determined by the preference to be accorded to warrants." *Illinois v. Gates*, 462 U.S. 213, 237 n.10 (1983) (quoting *United States v. Ventresca,* 380 U.S. 102, 109 (1965)). "This reflects both a desire to encourage use of the warrant process by police officers and a recognition that once a warrant has been obtained, intrusion upon interests protected by the Fourth Amendment is less severe than otherwise may be the case." *Id.*

1. *Suppression is unwarranted here because the new amendment to Rule 41(b) obviates the need for deterrence.*

On December 1, 2016, an amendment to Rule 41(b) became effective. Now, pursuant to Rule 41(b)(6), "[a]t the request of a federal law enforcement officer or an attorney for the government . . . 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 . . . ." *Id*. (emphasis added). This was not a "new" rule, but simply a clarification of the previous rule, which permitted the tracking of intangible items like electronic computer files. Nevertheless, because the rule now provides for a magistrate to issue this warrant, there is no need for deterrence here.

2. *Suppression is unwarranted here because the NIT did not violate the Fourth Amendment*.

Rule 41 violations fall into two categories: those involving constitutional violations and all others. *See United States v. Gerber,* 994 F.2d 1556, 1560 (11th Cir. 1993). A constitutional violation occurs only if the violation renders the search unconstitutional under the Fourth Amendment. *Id* at 1560. The Fourth Amendment demands three things of a search warrant: a warrant must be issued by a neutral magistrate; it must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and it must satisfy the particularity requirement. *Dalia*, 441 U.S. at 255. Those requirements are all met here.

Instead, citing *Levin*, the defendant's primary argument is that the Judge in the Eastern District of Virginia issued the NIT warrant in violation of Rule 41(b)(4) because his computer was located in the Middle District of Florida instead of the Eastern District of Virginia. However, the Fourth Amendment

does not impose a venue requirement for applying for a search warrant. Indeed, Rule 41 allows for extraterritorial searches. Rule 41(b)(2) through (b)(5) all describe situations in which the location of the search can be outside the district in which the issuing judge presides.

In addition, 18 U.S.C. § 2703(a) permits the issuing of search warrants to internet service providers by a "court of competent jurisdiction," and § 2711(3)(A)(i) defines that term to include a district court that "has jurisdiction over the offense being investigated." *Id*. Thus, venue is not a Fourth Amendment issue – it is a procedural one. *See Gerber,* 994 F.2d at 1559-60 (finding that a search conducted after the tenth day authorized by the warrant was not of a constitutional magnitude because "[t]he Fourth Amendment does not specify that search warrants contain expiration dates," and instead Rule 41 imposes that requirement).

Moreover, the individual privacy interests here were limited because the only NIT item used to support the residential search warrant was the defendant's IP address – something in which the defendant had no reasonable expectation of privacy. *Smith v. Maryland,* 442 U.S. 735, 743-44 (1979) (noting that the Supreme Court has "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.") Because an IP address is voluntarily turned over to a third party – the internet service provider – a person cannot expect privacy over that

IP address.[5] The defendant does not and cannot dispute that by accessing the Internet, even through the Tor, he gave others his IP address.[6]

3. *Suppression is Unwarranted for a Technical Violation of Rule 41(b).*

In the absence of a constitutional violation, "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." *United States v. Loyd,* 721 F.2d 331, 333 (11th Cir. 1983) (per curiam) (quoting *United States v. Sefanson*, 648 F.2d 1231, 1235 (9th Cir.1981)) (citations omitted). Neither prong is met here. First, there is no prejudice because all that was required to obtain the local search warrant was the defendant's IP address – something in which the

[5] The Eleventh Circuit has not decided whether a person has a reasonable expectation of privacy in an IP address, but has recognized case precedent on this issue from other circuits. *See Rehlberg v. Paulk*, 611 F.3d 828, 843 (11th Cir. 2010). *See also Penton v. United States*, 2013 WL 6009537 at *13 (M.D. Ala. Nov. 13, 2013) (collecting circuit cases that declined to recognize a Fourth Amendment privacy interest in IP addresses); and *United States v. Torres*, 2015 WL 1607985 at *1 (S.D. Ga. Apr. 7, 2015) (finding that "it is clear that Defendant had no constitutionally-protected privacy interest in either the IP address or the subscriber information held by Comcast.").

[6] The use of Tor does not create a reasonable expectation of privacy in IP addresses. *See Rivera*, Ex. 4 at 18, and *Werdene*, 2016 WL 3002376 at *8-10. ("a necessary aspect of Tor is the initial transmission of a user's IP address" to a third party. . . . [I]n order for a prospective user to use the Tor network[,] they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations.").

defendant had no reasonable expectation of privacy.

Second, the defendant cannot show that the FBI acted intentionally and with deliberate disregard of Rule 41(b). A review of the warrant application fails to show any deception, misrepresentation, or misdirection. The agent was candid about the challenges that the Tor network posed, specifically its ability to mask a user's physical location. NIT Warrant, ¶¶ 29, 31. The agent also stated that the NIT would be deployed "each time" that "any user" logged into Playpen "wherever" they were "located." *Id.* at ¶ 46. The FBI did not attempt to mislead the Magistrate Judge in any way as to the location of the activating computers or how the search and seizure would occur.

Accordingly, since the defendant did not suffer any prejudice and the agents did not act in deliberate disregard of Rule 41(b), suppression of the evidence is not warranted. *See United States v. Brown*, 569 F. App'x 759, 763 (11th Cir. 2014) (unpublished) (holding that an alleged Rule 41 violation did not merit suppression because obtaining a warrant from a state court did not constitute a clear violation of the rule, the defendant failed to show how the search prejudiced him, and the search was conducted in good faith); *United States v. Schumaker*, 479 F. App'x 878, 882-83 (11th Cir. 2012) (unpublished) (holding that defendant was not entitled to suppression of evidence recovered from his laptop and electronic devices because the defendant did not suffer prejudice and the government did not intentionally disregard Rule 41 when

the materials were reviewed after the 10-day period prescribed by the rule); *United States v. Gerber*, 994 F.2d 1556, 1559-61 (11th Cir. 1993) (holding that suppression was improper because the government did not intentionally disregard Rule 41 when it conducted a search after the search warrant had expired); *Loyd,* 721 F.2d at 332 (concluding that the magistrate's failure to certify the transcript of taped oral search warrant after the search had taken place did not merit suppression); *United States v. Comstock*, 805 F.2d 1194, 1207-08 (5th Cir. 1986) (applying *Loyd* and holding that non-compliance with Rule 41 did not warrant exclusion "simply because the constable has blundered."); *see also United States v. Lehder-Rivas*, 955 F.2d 1510 (11th Cir. 1992) (noting that suppression is appropriate if the magistrate abandoned his role as neutral arbiter, if the officers were dishonest or reckless in preparing the affidavit supporting the search warrant, or if the officers lacked an objectively reasonable belief that probable cause existed.).

4. The Leon *good faith exception applies because the FBI acted in good faith.*

"Courts generally should not render inadmissible evidence obtained by police officers acting in reasonable reliance upon a search warrant that is ultimately found to be unsupported by probable cause." *United States v. Martin*, 297 F.3d 1308, 1313 (11th Cir. 2002) (citing *United States v. Leon*, 468 U.S. 897, 922, (1984)). "The *Leon* good faith exception applies in all but four

limited sets of circumstances. The four sets of circumstances are as follows: (1) where 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) where the issuing magistrate wholly abandoned his judicial role in the manner condemned in; (3) where the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where, depending upon the circumstances of the particular case, a warrant is 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*. (internal citations and quotations omitted).

"The Leon good faith exception requires suppression 'only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.'" *Id*. (quoting *Leon*, 468 U.S. at 926). "The purpose of the exclusionary rule is to deter unlawful police misconduct; therefore, when officers engage in 'objectively reasonable law enforcement activity' and have acted in good faith when obtaining a search warrant from a judge or magistrate, the Leon good faith exception applies." *Id*. (quoting *Leon*, 468 U.S. at 919-920). "In the ordinary case, an officer cannot be expected to

question the magistrate's probable cause determination." *Leon*, 468 U.S. at 921. The application of this exception is based upon the "totality of the circumstances." *United States v. Taxacher*, 902 F.2d 867, 872 (11th Cir. 1990).

None of the four circumstances are present here. The first three circumstances do not apply on their face. The warrant was not "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 486 U.S. at 923. The fourth – that "a warrant is 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," also does not apply here. There is certainly no reason that the executing officers should have known that the magistrate erred when she signed the warrant – indeed the defendant does not even contest that the warrant affidavit established probable cause.

Instead, the defendant argues that the good faith exception does not apply at all because the warrant was void *ab initio*. The defendant relies on the Court's holding in *United States v. Levin*, --- F. Supp. 3d ---, No, 15-10271-WGI, 2016 WL 2596010 (D. Mass. May 5, 2016). But the continuing validity of the *Levin* decision has been widely questioned. For example, another defendant, citing *Levin*, raised the same argument in *United States v. Kneitel*, 8:16-cr-00023-MSS-JSS (M.D. Fla. Jan. 3, 2017) (Scriven, J.). The *Kneitel* Court held that "*Levin* has been subsequently called into question,

primarily because it relies on a 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)." *Id*. (citing*, United States v. Werdene*, --- F. Supp. 3d ---, No, 15-434, 2016 WL 3002376 at *14-20 (E.D. Pa. May 18, 2016)). Moreover, since *Levin* was decided, four other district courts in that same district – the District of Massachusetts – have held that the good faith exception did apply to the NIT warrant. *United States v. Tran*, No. 16-10010, 2016 WL 7468005 (D. Mass. Dec. 28, 2016); *United States v. Stepus*, No. 15-cr-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *United States v. Allain*, No. 15-cr-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *United States v. Anzalone*, No. 15-cr-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016). The decision in *Levin* is fully briefed and currently on appeal to the First Circuit Court of Appeals.

In fact, the vast majority of courts to consider this issue – at least 31 to date – have held that the good faith exception applied.[7] Only four courts out

[7] *United States v. Jeremy Hachey*, 5:16-cr-128 (E.D. Pa. Mar. 9, 2017); *United States v. Pawlak*, No. 16-CR-306, 2017 WL 661371 (N.D. Tex. Feb. 17, 2017); *United States v. Perdue*, No. 16-CR-305, 2017 WL 661378 (N.D. Tex. Feb. 17, 2017) (consolidated with *Pawlak*); *United States v. Kahler*, No. 16-CR-20551, 2017 WL 586707, (E.D. Mich. Feb. 14, 2017); *United States v. Deichert*, No. 5:16-cr-201, 2017 WL 398370 (E.D. N.C. Jan. 28, 2017); *United States v. Sullivan*, No. 1:16-cr-270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); *United States v. Kneitel*, No. 16-cr-23-MSS-JSS (M.D. Fl. Jan. 3, 2017); *United States v. Tran*, No. 16-10010, 2016 WL 7468005 (D. Mass. Dec. 28, 2016); *United States v. Dzwonczyk*, No. 15-CR-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016);

of at least 49 courts to issue decisions on the NIT warrant have held that the good faith exception did not apply.[8]

Exclusion of the evidence in this case would only serve to "punish the errors of judges and magistrates" and would not have any "appreciable" effect

---

United States v. Vortman, No. 16-cr-210, 2016 WL 7324987 (N.D. Cal. Dec.16, 2016); *United States v. Hammond*, No. 16-cr-102, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *United States v. Duncan*, No. 15-cr-414, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *United States v. Owens*, No. 16-CR-38-JPS, 2016 WL 7053195 (E.D. Wisc. Dec. 5, 2016); *United States v. Tippens, et. al.*, No. 16-CR-5110 (W.D. Wa. Nov. 30, 2016); *United States v. Stepus*, No. 15-cr-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *United States v. Libbey-Tipton*, No. 16-cr-236 (N.D. Ohio Oct. 19, 2016); *United States v. Scarbrough*, No. 16-cr-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016) (adopting Mag. Rep. and Rec.); *United States v. Allain*, No. 15-cr-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *United States v. Anzalone*, No. 15-cr-10347, 2016 WL 5339723(D. Mass. Sept. 22, 2016); *United States v. Broy*, No. 16-cr-10030, 2016 WL 5172853 (C.D. Il. Sept. 21, 2016); *United States v. Ammons*, No. 3:16-cr-00011, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); *United States v. Knowles*, No. 15-cr-875, 2016 WL 6952109 (D. S.C. Sept. 14, 2016); *United States v. Torres*, No. 16-cr-285, 2016 WL 4821223 (W.D. Tx. Sep. 9, 2016); *United States v. Henderson*, No. 15-cr-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Adams*, No. 16-cr-011, 2016 WL 4212079 (M.D. Fl. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 2:15-cr-266-CJB-KWR (E.D. La. Jul. 20, 2016); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Epich*, No.15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (unnecessary to reach the issue of Rule 41 compliance, suppression unwarranted); *United States v. Stamper*, No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

[8] *United States v. Croghan* (and *Horton*) (consolidated order), Nos. 15-cr-48;15-cr-51, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Workman*, No. 15-cr-397, 2016 WL 5791209 (D. Co. Sept. 6, 2016); *United States v. Arterbury*, No. 15-CR-182-JHP (N.D. Okla. May 17, 2016); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016).

on law enforcement. The actions of the FBI in this case are a studied effort to comply with the law and judicial authorization. The evidence against the defendant is substantial, and the United States would have no case if this Court were to suppress it. Thus, the "cost" of suppression would be letting a "guilty and possibly dangerous defendant[ ] go free" – something that "offends basic concepts of the criminal justice system." *Herring,* 555 U.S. at 141 (quoting *Leon,* 468 U.S. at 908).

II. THE RESIDENTIAL SEARCH WARRANT WAS VALID.

The defendant argues that the residential search warrant was invalid because it was tainted by the invalid NIT warrant. For the reasons stated above, the NIT warrant was valid, so the residential warrant was not "tainted." Therefore, the defendant's argument fails.

III. THE DEFENDANT'S VOLUNTARY NON-CUSTODIAL INTERVIEW WITH LAW ENFORCEMENT SHOULD NOT BE SUPPRESSED.

The Supreme Court in *Miranda* "established that custodial interrogation cannot occur before a suspect is warned of [his] rights against self-incrimination." *United States v. Newsome*, 475 F.3d 1221, 1224 (11th Cir. 2007). Pre-custodial questioning, in contrast, does not require *Miranda* warnings. *United States v. Street*, 472 F.3d 1298, 1309 (11th Cir. 2006).

"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." *United States v. Street*, 472 F.3d 1298, 1309 (11th Cir. 2006). The "initial step" in determining whether a person was in "custody" under *Miranda* "is to ascertain whether, in light of the objective circumstances of the interrogation" and the totality of all the circumstances, "a reasonable person would have felt that he or she was not at liberty to terminate the interrogation and leave." *Howes v. Fields*, 132 S. Ct. 1181, 1189, (2012) (alterations and quotation marks omitted). An interviewee's "status as a suspect, and the coercive environment that exists in virtually every interview by a police officer of a crime suspect," does not automatically create a custodial situation. *United States v. Muegge*, 225 F.3d 1267, 1270 (11th Cir. 2000) (quotation marks omitted).

"One of the factors a court should consider when determining whether the defendant was 'in custody' is the location of questioning." *United States v. Matcovich*, 522 F. App'x 850, 851 (11th Cir. 2013) (citing *Howes*, 132 S. Ct. at 1189). Although not dispositive, "courts 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." *United States v. Brown*, 441 F.3d 1330, 1348 (11th Cir.2006). Courts may also consider whether a defendant was "unambiguously advis[ed] . . . that he is free to leave and is not in custody." *Id*. at 1347. This is a "powerful factor" that "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.* (quotation marks omitted).

Other relevant factors "includ[e] whether the officers brandished weapons, touched the suspect, or used language or a tone that indicated that compliance with the officers could be compelled," *Street*, 472 F.3d at 1309 (quotation marks omitted), as well as "the duration of the questioning, statements made during the interview, the presence of physical restraints during questioning, and 'the release of the interviewee at the end of the questioning,'" *Matcovich*, 522 F. App'x at 851 (quoting *Howes*, 132 S. Ct. at 1189).

Here, the defendant was not "in custody." The two critical factors – the unambiguous statement that the defendant did not need to answer questions, and the location of the interview – weigh heavily against the defendant. First, the interview occurred at the defendant's home on his back lanai. *See Brown*, 441 F.3d at 1348 ("courts 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.")

Second, FBI agents informed Caswell, clearly and repeatedly, that he was free to leave at any time and did not have to answer any questions. Agents told Caswell that he was "not under arrest" and that he "could leave at

any time. And any time, you can stop talkin' to - - you can say, 'Bunch, Zac, I'm done talkin' to you." The defendant acknowledged that he understood, stating that "I watch the shows." The agent again told Caswell he could "walk away" and specified that "if you wanna walk out your lanai, hop the fence and go, I'll wave [sic] to ya." The agent continued that "if you have to get up, let me know. Or if you wanna leave, let me know." This second factor is "powerful" 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." *Brown*, 441 F.3d 1330, 1347.

In addition to those two critical and dispositive factors, the other relevant factors show that the restrictions on Caswell's freedom did not rise to the degree associated with formal arrest. *Minnesota v. Murphy*, 465 U.S. 420 (1984); *see also* ELEVENTH CIRCUIT CRIMINAL HANDBOOK at § 151(b). The agents did not brandish weapons or touch the suspect during the interview, nor did they use restraints. Moreover, the language and tone used during the interview was conversational and non-confrontational – there was nothing to indicate that compliance could or would be compelled. Finally, the defendant was, in fact, released at the end of questioning. All of these factors show that the defendant was not "in custody" for *Miranda* purposes.

CONCLUSION

For the preceding reasons, the defendant's motion to suppress should be denied.

Respectfully submitted,

W. STEVEN MULDROW
Acting United States Attorney

By: *s/Charles D. Schmitz*

CHARLES D. SCHMITZ
Assistant United States Attorney
USAO No. 159
2110 First Street, Suite 3-137
Ft. Myers, Florida 33901
Telephone: (239) 461-2200
Facsimile: (239) 461-2219
E-mail: Charles.Schmitz@usdoj.gov

U.S. v. DAVID CASWELL **Case No. 2:16-cr-134-FtM-29MRM**

CERTIFICATE OF SERVICE

I hereby certify that on March 20, 2017, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to the following:

Gerald Thomas Berry, Esq.
JBerry@JBerryLaw.com

s/ Charles D. Schmitz
Charles D. Schmitz
Assistant United States Attorney