UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	CASE NO. 3:15-cr-05351-RJB ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS EVIDENCE

These matters come before the Court on Defendant's Motion to Suppress Evidence (Dkt. 26) and Defendant's Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Dkt. 65). The Court has considered the parties' responsive briefing and the remainder of the file herein, as well as the testimony of FBI Special Agent Daniel Alfin and Christopher Soghoian, Principal Technologist for the Speech and Technology Project at the American Civil Liberties Union, elicited at an evidentiary hearing held on January 22, 2016. Dkt. 47, 69, 90, 94, 111. Having orally denied Mr. Michaud's motion for a *Franks* hearing (Dkt. 135), the sole issue before the Court, raised by both of Mr. Michaud's motions, is whether to suppress evidence of what Mr. Michaud argues is fruit of an unreasonable search. At oral argument, the parties agreed

that the Court should decide the issue based on the submitted record, as supplemented by the testimony adduced at the hearing. *See* Dkt. 135.

I. FACTUAL BACKGROUND

a. Website A

Mr. Jay Michaud, a resident of Vancouver, Washington, is charged with receipt and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), (a)(4), (b)(1), and (b)(2). Dkt. 117. The charges against Mr. Michaud stem from Mr. Michaud's alleged activity on "Website A," a website that, according to the FBI, was dedicated to the advertisement and distribution of child pornography. Dkt. 47-5, at ¶¶14-16. Website A was created in August of 2014, and by the time that the FBI shut the site down, on March 4, 2015, Website A had over 200,000 registered member accounts and 1,500 daily visitors, making it "the largest remaining known child pornography hidden service in the world." Dkt. 47-1, at ¶19; Dkt. 50-1, at ¶3.

According to the three warrant applications submitted in this case, the main page of the site featured a title with the words, "Play Pen." Dkt. 47-1, at ¶¶12. *See also* Dkt. 47-5, at ¶¶18-37; Dkt 47-2, at ¶¶11-21. *See also* Dkt. 90-1, at 2. The main page, which required users to login to proceed, also featured "two images depicting partially clothed prepubescent females with their legs apart." *Id*. Text on the same page read, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." *Id*. "No cross-board reposts," appeared to prohibit the reposting of material from other websites, while ".7z preferred," referred to a preferred method of compressing large files. *Id*. After logging in, registered users would next view a page with hyperlinks to forum topics, the clear majority of which advertise child pornography. *Id*., at ¶¶14-18. *See also* Dkt. 65-2, at 1-4.

b. The Title III Warrant

On February 20, 2015, agents from the Federal Bureau of Investigation executed a Title III warrant to intercept the communications of Website A. Dkt. 47-5, at ¶4 and pp. 57-62. Website A operated on the Tor network, a publicly available alternative internet service that allows users to mask identifying information, such as Internet Protocol ("IP") addresses. *Id*., at ¶¶18-36. For approximately 14 days, from February 20, 2015 through March 4, 2015, the FBI administered Website A from a government-controlled computer server located in Newington, Virginia, which forwarded a copy of all website communications, through the server, to FBI personnel in Linthicum, Maryland. Dkt. 47-1, at ¶30; Dkt. 47-5, ¶¶38, 52 and p. 60. Based on the authority of the Title III warrant, the FBI captured communications of users accessing Website A, including user "Pewter." The FBI apparently did not post any new content but allowed registered users to access the site and to continue to post content. *See id*.

c. The NIT Warrant

While controlling Website A, the FBI sought to identify the specific computers, and ultimately the individuals, accessing the site, by deploying a network investigating technology ("NIT") that "cause(d) 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, [and] other information[.]" Dkt. 47-1, at 34. Prior to deploying the NIT, on February 20, 2015 the FBI sought and obtained a warrant ("the NIT Warrant"), which was issued by a magistrate judge in the Eastern District of Virginia. *Id*. The NIT Warrant cover sheet reads as follows:

> "An application by a federal law enforcement officer . . . requests the search of the following person of property located in the ____Eastern___ District of ___Virginia___ (*identify the person or describe the property to be searched and give its location)*:
> See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See Attachment B[.]" Dkt. 47-1, at 39.

Attachment A reads as follows:

Attachment A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers below.

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL – [omitted]— which will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization. *Id.*, at 37.

Attachment B reads as follows:

Attachment B

Information to be Seized

From any "activating" computer described in Attachment A:

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 data from that 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;

that is evidence of violations of . . . [child pornography-related crimes]. *Id*., at 38. Both Attachment A and Attachment B, which the NIT Warrant incorporated, are identical in content to the attachments submitted in the warrant application. *Id*., at 4, 5, 37, 38.

d. Warrant issued in the Western District of Washington ("the Washington Warrant")

After obtaining the NIT warrant, the FBI deployed the NIT, obtaining the IP address and other computer-related information connected to a registered user, "Pewter," who allegedly accessed Website A for 99 hours between October 31, 2014 and March 2, 2015. Dkt. 47-2, at ¶26. "Pewter" had apparently accessed 187 threads on Website A, most related to child pornography. *Id*., at ¶27. With the IP address in hand, the FBI ultimately ascertained the residential address associated with "Pewter," an address at which Mr. Michaud resided, in Vancouver, Washington. *Id*., at ¶¶35, 36. A magistrate judge in the Western District of Washington issued a warrant to search that address, and the FBI subsequently seized computers and storage media allegedly containing contraband. *See generally, id*.

e. Evidentiary testimony of SA Alfin and Dr. Christopher Soghoian

SA Alfin's testimony explained how the NIT was deployed against Mr. Michaud. While the FBI administered Website A from a government-controlled computer, between February 20, 2015 and March 4, 2015, a registered user, "Pewter," logged into Website A and accessed a forum entitled, "Preteen videos—girls HC." (HC stands for "hardcore.") The FBI setup the NIT so that accessing the forum hyperlink, not Website A's main page, triggered the automatic deployment of the NIT from the government-controlled computer in the Eastern District of Virginia, to Pewter's computer in Vancouver, Washington, where the NIT collected the IP address, MAC address, and other computer-identifying information, and relayed that information back to the government-controlled server in the Eastern District of Virginia, after which the information was forwarded to FBI personnel for data analysis.

SA Alfin also explained a discrepancy in the content of Website A's main page. While the warrant application for the NIT describes a main page featuring two prepubescent females with legs spread apart, Dkt. 47-1, at ¶12, by the time that the FBI submitted the warrant application, on February 20, 2015, the main page had been changed to display only one young female with legs together. *Compare* Dkt. 90-1, at 2 and Dkt. 90-1, at 4. According to SA Alfin, the main page changed several hours prior to the arrest of a Website A administrator, in the early evening hours of February 19, 2015. After the arrest, SA Alfin viewed Website A and other material on the administrator's computer, at which point SA Alfin saw the newer version of Website A's main page but did not notice the picture changes. The balance of Website A's focus on child pornography apparently remained unchanged, in SA Alfin's opinion. The new picture also appears suggestive of child pornography, especially when considering its placement next to the site's suggestive name, Play Pen.

Dr. Christopher Soghoian, testifying on behalf of Mr. Michaud, explained how the Tor network functions and theorized about how the NIT may have been deployed.

II. DISCUSSION

Mr. Michaud raises two[1] primary Fourth Amendment issues: whether deploying the NIT from the Eastern District of Virginia, to Mr. Michaud's computer, located outside that district, exceeded the scope of the NIT Warrant's authorization; and whether the NIT Warrant lacks particularity and amounts to a general warrant. In addition to those constitutional issues, Mr. Michaud raises the issue of a statutory violation, that is, whether the NIT Warrant violates Fed. R. Crim. P. Rule 41(b). Based on those issues, Mr. Michaud requests suppression of evidence secured through the NIT and all fruits of that search.

a. Whether deploying the NIT to a computer outside of the Eastern District of Virginia exceeded the scope of the NIT Warrant's authorization.

Mr. Michaud argues that the NIT Warrant authorized deployment of the NIT only to computers within one geographical location, the Eastern District of Virginia. Dkt. 65, at 15-17. Dkt. 139, at 3, 4. He asserts that because the FBI deployed the NIT to Mr. Michaud's computer, located outside of that district, the search and seizure exceeded the scope of the NIT Warrant. *Id*.

The Fourth Amendment to the United States Constitution provides that "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." If the execution of a search or seizure exceeds the scope of a warrant, the subsequent search or seizure is

---

[1] In his motion for a *Franks* hearing, Mr. Michaud raised a third constitutional issue, challenging the probable cause underlying the NIT Warrant, which the Court denied at oral argument. Dkt. 135. *See* Dkt. 65, at 5-15. However, even if the NIT Warrant was not supported by probable cause, as Mr. Michaud argued, reliance on the NIT Warrant was objectively reasonable, *see supra*, so suppression is not warranted. *U.S. v. Needham*, 718 F.3d 1190, 1194 (9th Cir. 2013).

unconstitutional. *Horton v. California*, 496 U.S. 128, 140 (1990). Whether a search or seizure exceeds the scope of a warrant is an issue that is determined "through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search." *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir 2007)(*internal quotations and citations omitted*).

Mr. Michaud's argument requires an overly narrow reading of the NIT Warrant that ignores the sum total of its content. While the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context:

> "An application by a federal law enforcement officer . . . requests the search of the following person of property located in the ____Eastern___ District of ___Virginia___ (*identify the person or describe the property to be searched and give its location)*:
> See Attachment A[.]" Dkt. 47-1, at 39.

The warrant explicitly invites the magistrate judge to "give its location" in the blank space provided, wherein the phrase, "See Attachment A," is inserted. Attachment A, subtitled "Place to be Searched," authorizes deployment of the NIT to "all activating computers," defined as "those of any user or administrator who logs into [Website A] by entering a username and password." *Id*. Attachment A refers to the Eastern District of Virginia as the location of the government-controlled computer server from which the NIT is deployed. *Id*. A reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.

The warrant application reinforces this interpretation, which is objectively reasonable. The warrant application, when detailing how the NIT works, explains that the NIT "may cause

an activating computer—*wherever located*—to send to a computer controlled by or known to the government [in the Eastern District of Virginia], network level messages *containing information that may assist in identifying* the computer, *its location*, and other information[.]" Dkt. 47-1, at ¶46 (emphasis added). The execution of the NIT Warrant is also consistent with and supports this interpretation. *See* Dkt. 47-5, at ¶¶13-18. Because this interpretation is objectively reasonable, execution of the NIT Warrant consistent with this interpretation should be upheld, even if there are other possible reasonable interpretations. *Bergquist v. County of Cochise*, 806 F.2d 1364 (9th Cir. 1986) (*abrogated on other grounds by City of Canton, Ohio v. Harris*, 489 U.S. 378 (1989).

b. Whether the NIT Warrant lacks specificity and amounts to a general warrant.

Mr. Michaud argues in the alternative that if the NIT Warrant did not limit the NIT's deployment to computers within one geographic location, the Eastern District of Virginia, the NIT Warrant is also unconstitutional because it lacks specificity and amounts to a general warrant. Dkt. 65, at 17; Dkt. 111, at 20.

Whether a warrant lacks specificity depends on two factors, particularity and breadth. "Particularity means the 'warrant must make clear . . . exactly what it is that he or she is authorized to search for and seize.'" *United States v. SDI Future Health, Inc.*., 568 F.3d 684, 702 (9th Cir. 2009)(quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9th Cir. 1991). Warrants do not lack particularity where they "describe generic categories of items . . . if a more precise description of the items . . . is not possible." *Id*. (citing to *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986)). "Breadth" inquires as to whether the scope of the warrant exceeds the probable cause on which the warrant is based. *Id*.

As a threshold matter, it appears that even if Mr. Michaud was correct in arguing that the NIT Warrant is unconstitutional because it is a general warrant, suppression may not be required

because the officers acted in good faith when executing the warrant. *See supra*, II(c)(3). *See also, United States v. Negrete Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992) (citing to *United States v. Leon*, 468 U.S. 897 (1984)). The NIT Warrant does not, however, lack sufficient specificity. The warrant states with particularity exactly what is to be searched, namely, computers accessing Website A. Dkt. 47-1, at 37. According to the warrant application upon which the NIT Warrant was issued, Website A is unmistakably dedicated to child pornography. Although the FBI may have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that does not negate particularity, because it would be highly unlikely that Website A would be stumbled upon accidentally, given the nature of the Tor network.

The second factor, breadth, considers whether the NIT Warrant exceeded the probable cause on which it was issued. While the warrant application certainly provides background facts not found in the NIT Warrant itself, *compare* Dkt. 47-1, at 2-36 and Dkt. 47-1, at 37-40, the NIT Warrant does not authorize anything beyond what was requested by the warrant application. In fact, the NIT Warrant language found in Attachment A and Attachment B is identical to the scope of the warrant requested. *Id*., at 4, 5, 37, 38. Both the particularity and breadth of the NIT Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant.

c. Whether the NIT Warrant violates Fed. R. Crim. P. Rule 41(b).

Concerning Fed. R. Crim. P. Rule 41(b), Mr. Michaud makes three primary arguments: (1) the NIT Warrant violates the plain text of Rule 41(b), (2) the Rule 41(b) violation requires suppression, because the violation was the result of an intentional and deliberate disregard of Rule 41(b), and results in prejudice to Mr. Michaud, and (3) the good faith exception does not "save" the Rule 41(b) violation because it does not apply. Dkt. 26, at 8-16; Dkt. 69, at 3-11.

1. Plain text of Rule 41(b).

According to Mr. Michaud, the NIT Warrant violates the general provision of Rule 41(b), subdivision (b)(1), because the rule prohibits the magistrate judge in the Eastern District of Virginia from issuing a warrant to search or seize a computer outside of her district, including Vancouver, Washington. Dkt. 26, at 11-13. Mr. Michaud also argues against the applicability of the rule's other subdivisions, which carve out exceptions for searches outside of the district. Dkt. 26, at 13, 14.

18 U.S.C. § 3103, which governs the grounds for issuing search warrants, directly incorporates Rule 41(b). Subdivision (b)(1) states the general rule, that "a magistrate with authority in the district . . . has the authority to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). Exceptions apply where a person or property "might move or be moved outside the district before the warrant is executed," subdivision (b)(2), when federal law enforcement investigates terrorism, subdivision (b)(3), when a tracking device installed within the district travels outside the district, subdivision (b)(4), and where the criminal activities occur on a United States territory, commonwealth, or other location under the control of the United States other than a state, subdivision (b)(5).

Rule 41(b) is to be applied flexibly, not rigidly. *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992). In *United States v. New York Tel. Co.*, 434 U.S. 159 (1977), the Supreme Court addressed the general relationship of technology and Rule 41, concluding that Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause." *Id.*, at 169. The *New York Tel. Co.* court noted that a flexible reading of Rule 41 is reinforced by Fed. R. Crim. P. 57(b), which provides that in the absence of controlling law, "a judge may regulate practice in any manner consistent with federal law, these

rules and the local rules[.]" *Id*., at 170.[2] Although *New York Tel. Co.* addressed a now-superseded subdivision of Rule 41 and a different technology, the pen register, the flexibility applied to Rule 41 has since been applied to subsection (b) of Rule 41. *See, e.g., Koyomejian*, 970 F.2d at 542.

In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT Warrant technically violates the letter, but not the spirit, of Rule 41(b). The rule does not directly address the kind of situation that the NIT Warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location. In this context, and when considering subdivision (b)(1), a cogent, but ultimately unpersuasive argument can be made that the crimes were committed "within" the location of Website A, Eastern District of Virginia, rather than on personal computers located in other places under circumstances where users may have deliberately concealed their locations. However, because the object of the search and seizure was Mr. Michaud's computer, not located in the Eastern District of Virginia, this argument fails. In a similar vein, a reasonable, but unconvincing argument can be made that subdivision (b)(2) applies, given the interconnected nature of communications between Website A and those who accessed it, but because Mr. Michaud's computer was not ever physically within the Eastern District of Virginia, this argument also fails.

---

[2] Although not argued by the parties, a flexible interpretation of Rule 41(b) that accounts for changes in technology may also reconcile Rule 41(b) with 18 U.S.C. § 3103a, which provides that "[I]n addition to the grounds for issuing a warrant [under Rule 41(b)], a warrant may be issued . . . for . . . any property that constitutes evidence of a criminal offense." As the parties appeared to agree at oral argument, § 3103a was enacted to codify the elimination of the mere evidence rule overturned in *Warden v. Hayden*, 387 U.S. 294 (1967), but neither party offered a satisfactory explanation to reconcile § 3103a with § 3103 and Rule 41(b).

Finally, applying subdivision (b)(4), which allows for tracking devices installed within one district to travel to another, stretches the rule too far. If the "installation" occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because Mr. Michaud never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on Mr. Michaud's computer, applying the tracking device exception again fails, because Mr. Michaud's computer was never physically located within the Eastern District of Virginia. The Court must conclude that the NIT Warrant did technically violate Rule 41(b), although the arguments to the contrary are not unreasonable and do not strain credulity.

2. Prejudice to Mr. Michaud and intentional and deliberate disregard of Rule 41(b).

Rule 41(b) violations are categorized as either fundamental, when of constitutional magnitude, or technical, when not of constitutional magnitude. *Negrete-Gonzales*, 966 F.2d at 1283. As concluded above, the NIT Warrant did not fail for constitutional reasons, but rather was the product of a technical violation of Rule 41(b). Sec. II(c)(1). In cases where a technical Rule 41(b) violation occurs, courts may suppress where a defendant suffers prejudice, "in the sense that the search would not have occurred . . . if the rule had been followed," or where law enforcement intentionally and deliberately disregarded the rule. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (citing to *United States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005)).

In this case, suppression is not warranted on the basis of the technical violation of Rule 41(b), because the record does not show that Mr. Michaud was prejudiced or that the FBI acted intentionally and with deliberate disregard of Rule 41(b). First, considering the prejudice, Mr. Michaud would have the Court interpret the definition of prejudice found in *Weiland* and

elsewhere, "in the sense that the search would not have occurred . . . if the rule had been followed," to mean that defendants suffer prejudice whenever a search occurs that violates Rule 41(b). This interpretation makes no sense, because under that interpretation, all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Such an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation. Tracing the origin of the definition used in *Weiland* to its early use in the Ninth Circuit yields a more sensible interpretation of the well-established definition: "in the sense that the search would not have occurred . . . if the rule had been followed" suggests that courts should consider whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the defendant did not suffer prejudice. *See United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980).

Applying that interpretation here, Mr. Michaud did not suffer prejudice. Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

Mr. Michaud also fails to show that the FBI acted intentionally and with deliberate disregard of Rule 41(b). Mr. Michaud's arguments to the contrary rely only on thin inferences, which are insufficient. Mr. Michaud argues that the Rule 41(b) violation of the NIT Warrant, which was predicated on the FBI's warrant application, was so obvious that the mere submission of the warrant application shows an intent to disregard the rule. The NIT Warrant did technically violate Rule 41(b), but reasonable, although unavailing arguments can be made to the contrary. *See infra*, II(a) and (c)(2). Mr. Michaud points to one opinion by a magistrate judge, who denied a similar warrant application seeking authorization to search "Nebraska and elsewhere," as evidence of intent and deliberate disregard, but that magistrate judge, who sits in one of ninety-four judicial districts, ruled on an unsettled area of the law where there is no controlling circuit or Supreme Court precedent. *See United States v. Cottom* Findings and Recommendations, Nebraska CR13-0108JFB. *See also*, Dkt. 69-1; Dkt. 111-2. Mr. Michaud also argues intent and deliberate disregard are shown by that the fact that the Government has elsewhere argued that Rule 41(b) should be amended to account for changes in technology, but this argument also fails, given that reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in uncharted territory. *See also*, Fed. R. Crim. P. 57(b).[3]

3. Good faith.

Mr. Michaud also argues that, because the NIT Warrant violated Rule 41(b) and the Constitution, suppression is required because the good faith exception does not apply; and that the FBI did not execute the NIT Warrant in good faith.

---

[3] It appears clear that Fed. R. Crim. P. 41 or 18 U.S.C. § 3103 should be modified to provide for issuance of warrants that involve modern technology. Furthermore, said rule only applies to magistrate judges and state judges, and does not address limits on warrants issued by other federal judicial officers.

Where a warrant is executed in good faith, even if the warrant itself is subsequently invalidated, evidence obtained need not be suppressed. *United States v. Leon*, 468 U.S. 897, 922 (1984). Warrants may be invalidated for technical or fundamental (constitutional) violations. *See id.*, at 918 (technical violation) and *Negrete-Gonzales*, 966 F.2d at 1283 (constitutional violation). Whether a warrant is executed in good faith depends on whether reliance on the warrant was objectively reasonable. *Id.*, at 922.

"'Searches pursuant to a warrant will rarely require any deep inquiry into reasonableness.'" *Leon*, at 922 (quoting *Illinois v. Gates*, 462 U.S., 213, 267 (1983)). Nonetheless, reliance on the NIT Warrant was objectively reasonable. *See infra,* II(a) and (c)(2). Mr. Michaud's argument that the good faith exception does not apply, because *Weiland* overrules *Negrete-Gonzales*, which explicitly analyzed good faith in the context of a Rule 41(b) violation, is unavailing. Although the *Weiland* court makes no mention of good faith, it did not reach the issue, because it affirmed a lower court's finding that suppression was not appropriate where there was no showing of a Rule 41(b) violation of constitutional magnitude, prejudice to the defendant, or intentional and deliberate disregard of the rule. *Id.*, at 1072. Because reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted.

III. CONCLUSION

"The Fourth Amendment incorporates a great many specific protections against unreasonable searches and seizures. The contours of these protections in the context of computer searches pose difficult questions." *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006)(*internal quotations and citations omitted*). What was done here was ultimately reasonable. The NIT Warrant was supported by probable cause and

particularly described the places to be searched and the things to be seized. Although the NIT Warrant violated Rule 41(b), the violation was technical in nature and does not warrant suppression. Mr. Michaud suffered no prejudice, and there is no evidence that NIT Warrant was executed with intentional and deliberate disregard of Rule 41(b). Instead, the evidence shows that the NIT Warrant was executed in good faith. Mr. Michaud's motions to suppress should be denied.

* * *

THEREFORE, it is HEREBY ORDERED that Defendant's Motion to Suppress Evidence (Dkt. 26) is DENIED. Defendant's Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Dkt. 65) is DENIED.

The Clerk is directed to send uncertified copies of this Order to all counsel of record and to any party appearing *pro se* at said party's last known address.

Dated this 28th day of January, 2016.

ROBERT J. BRYAN
United States District Judge