United States v. Beau Brandon Croghan

United States District Court for the Southern District of Iowa

September 19, 2016., Decided

1:15-cr-48 1:15-cr-51

Reporter
2016 U.S. Dist. LEXIS 127479

UNITED STATES OF AMERICA, Plaintiff, v. BEAU BRANDON CROGHAN, Defendant. UNITED STATES OF AMERICA, Plaintiff, v. STEVEN SHANE HORTON, Defendant.

Notice: Decision text below is the first available text from the court; it has not been editorially reviewed by LexisNexis. Publisher's editorial review, including Headnotes, Case Summary, Shepard's analysis or any amendments will be added in accordance with LexisNexis editorial guidelines.

Core Terms

suppression, user, website, magistrate judge, law enforcement, computers, tracking device, activating, Warrants, installed, site, server, track, Resistance, deployed, good faith, authorize, privacy, void, identifying information, authority to issue, search warrant, issuance, searched, network, logged, seized, reasonable expectation of privacy, provides, reckless disregard

Opinion

[*1] ORDER ORDER Before the Court are two Motions to Suppress, one filed by Defendant Beau Croghan in

Case No. 1:15-cr-48 ("Croghan"), and one filed by Defendant Steven Horton in Case No. 1:15-

cr-51 ("Horton"). Croghan Clerk's No. 33; Horton Clerk's No. 45. The Government filed an

identical resistance brief in each case. Croghan Clerk's No. 36; Horton Clerk's No. 49. Because

the facts leading to each Defendant's arrest are fundamentally the same, the Court considers the

Motions to Suppress together. And, because the facts are undisputed, the Court agrees with the

parties that no hearing is necessary. The matters are, therefore, fully submitted.

I. FACTUAL BACKGROUND

In approximately September 2014, the Federal Bureau of Investigation ("FBI") began investigating a child pornography website known as "Playpen." NIT Warrant1¶ 11. Playpen existed as a "hidden service" on the "Tor" network, which is designed to protect user anonymity by obscuring identifying information such as the user's IP address.2*Id.* ¶ 10. Because "hidden services" are not publically indexed or searchable, a user must both connect to Tor and know the specific Tor-based web address of a particular site to gain access. *Id.*

During the course **[*2]** of its investigation, the FBI connected to the Playpen website and discovered that it appeared to be dedicated to advertising and distributing child pornography. *Id.* ¶¶ 11-12. In December 2014, a foreign law enforcement agency advised the FBI that it had discovered the actual IP address of the Playpen server and that such server was located in Lenoir, North Carolina. *Id.* ¶ 28. In January 2015, the FBI obtained and executed a search warrant whereby it seized the Playpen website server. *Id.* Hoping to locate and identify visitors to the site, the FBI placed a complete copy

of the Playpen website, including all of the child pornography on the website, on a government-controlled server located in Newington, Virginia.

Id.; *see also* Gov't Resistance Br. at 2. On February 19, 2015, the FBI arrested the suspected

1 Throughout this Order, the Court will refer to the search warrant obtained in the Eastern District of Virginia (Croghan Clerk's No. 33-2; Horton Clerk's No. 45-2) as the "NIT Warrant." In the affidavit filed in support of the NIT Warrant, the Playpen website is referred to interchangeably as "TARGET WEBSITE" or "WEBSITE A."

2 The Tor network "is a group of volunteer-operated servers that allows people **[*3]** to improve their privacy and security on the internet" by allowing users to connect to websites "through a series of virtual tunnels rather than [by] making a direct connection." *See* https://www.torproject.org/about/overview.html.en (last visited Sept. 12, 2016). Thus, the Tor network "prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and [] lets the user access sites which could otherwise be blocked." NIT Warrant ¶ 8.

administrator of the Playpen website and "assumed administrative control" of it. NIT Warrant ¶ 30.

On February 20, 2015, the FBI submitted an application for and affidavit in support of a search warrant to Eastern District of Virginia Magistrate Judge Theresa Carroll Buchanan. *See generally* NIT Warrant. The affidavit provided that the FBI intended to continue operating the Playpen website from its own server for a period of time not to exceed 30 days in an attempt to identify users of the site. *Id.* ¶ 30. Because the site utilized the Tor network to mask user identify information, the FBI requested that Magistrate Judge Buchanan authorize use of a "Network Investigative Technique" ("NIT") whereby **[*4]** the FBI would insert computer software into the Playpen website that would assist it in "locat[ing] and apprehend[ing] the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children" by accessing the Playpen website. *Id.* Once installed on the Playpen website on the government-controlled server, the NIT would be deployed to the computer of any user who visited the Playpen website and entered a user name and password. *Id.* ¶¶ 31-34; Croghan Br. at 7 (noting that the NIT would be deployed to "'any user' who logged into the site with a username and password, regardless of their physical location, whether or not they were using the site's chat features, or viewing child pornography"). The NIT would then force the "activating" computer to transmit information back to the FBI, including: the IP address of the activating computer; the date and time the NIT determined the IP address; a unique identifier generated by the NIT to distinguish data from different activating computers; the type of operating system running on the activating computer, including type, version, and architecture; information on whether the NIT had already been delivered to the activating computer; **[*5]** the "host name" of the activating computer; the operating system used by the activating computer; and the Media Access Control

("MAC") address of the activating computer. NIT Warrant ¶ 34. Magistrate Judge Buchanan approved the warrant and authorized the FBI to deploy the NIT for 30 days. *See generally id.* She further granted a request by the Government to delay notice of the search "until 30 days after any individual accessing the [Playpen site] has been identified to a sufficient degree as to provide notice" under *18 U.S.C. § 3103(a)(b)* and *Federal Rule of Criminal Procedure 41(f)(3)*.

Id. ¶¶ 38-41.

The Government began deploying the NIT on February 20, 2015, and continued to do so until March 4, 2015, at which time it took the Playpen website offline. Gov't Resistance Br. at 2. On July 17, 2015, law enforcement obtained a search

warrant for Beau Croghan's residence in Council Bluffs, Iowa. Croghan Clerk's No. 33-3. Law enforcement obtained a search warrant for Steven Horton's residence in Glenwood, Iowa on August 5, 2015.3Horton Clerk's No. 45-2. The affidavits submitted in support of each of the Iowa Warrants relied primarily on information collected from the NIT. In particular, each affidavit described the Playpen website, its existence on the Tor network, **[*6]** and the authorization for the NIT from the Eastern District of Virginia. The affidavits recounted that the NIT had yielded specific user names and IP addresses, and that subsequent investigation using public records and administrative subpoenas to Internet Service Providers ("ISPs") had associated the identified IP addresses with Croghan, Horton, and their specific residences. While executing the warrants, law enforcement seized evidence from each Defendant's home, eventually culminating in both men being indicted for accessing or attempting to access child pornography in violation of *18 U.S.C. § 2252(a)(5)(B)*.

3 The Court will collectively refer to the warrants executed at Defendants'

residences as the "Iowa Warrants."

II. LAW AND ANALYSIS

Defendants urge that all evidence discovered by virtue of and flowing from the NIT warrant must be suppressed. In particular, they argue: (1) the NIT warrant was issued in violation of *Federal Rule of Criminal Procedure 41*; (2) as a result of the *Rule 41* violation, evidence obtained by use of the NIT must be suppressed; (3) evidence obtained as a result of the Iowa Warrants must also be suppressed because the probable cause supporting their issuance was derived solely from evidence collected by virtue of the NIT; **[*7]** and (4) no good faith exception is applicable to avoid suppression. The Government counters: (1) that the NIT warrant complied with *Rule 41*; (2) that even if *Rule 41* was violated, suppression is not warranted; and (3) that the good faith exception applies in any event.

The Court notes that the NIT Warrant at issue in this case has resulted in a great deal of litigation across the country. The numerous district courts to consider motions similar to the present Motions to Suppress have reached varying conclusions on the legal issues at play. At least two courts have concluded that the NIT Warrant was unlawfully issued and suppressed all fruits of it. *See, e.g., United States v. Levin*, No. 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-cr-182, Clerk's No. 42 (N.D. Okla. Apr. 25, 2016). Several others have found that while the NIT Warrant may have been issued unlawfully, suppression was not warranted, either under the exclusionary rule in general or pursuant to the

*Leon*4good faith exception. *See United States v. Torres*, No. 5:16-cr-285, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); *United States v. Henderson*, No. 15-cr-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Adams*, No. 6:16-cr-11, 2016 WL 4212079 (N.D. Fla. Aug.

4 *See United States v. Leon, 468 U.S. 897 (1984)*.

10, 2016); *United States v. Acevedo-Lemus*, No. 15-00137, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016);

United States v. Epich, No. 15-cr-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Michaud*, No 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). And, at least four decisions, three from the Eastern District of Virginia and one from the Western District of Arkansas, have concluded that the magistrate judge possessed adequate authority to issue the NIT Warrant under *Rule 41* **[*8]** such that there was no legal violation that would require suppression. *See, e.g., United States v. Jean*, No. 5:15-cr-50087, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Eure*, No 2:16cr43, 2016 WL 4059663

(E.D. Va. July 28, 2016); *United States v. Matish*, No. 4:16cr16, 2016 WL 3545776 (E.D. Va. June 23, 2016);

United States v. Darby, No. 2:16cr36, 2016 WL 3189703 (E.D. Va. June 3, 2016). A. *Did the NIT Warrant Comply With Rule 41*

The *Federal Magistrates Act* provides that "[e]ach United States magistrate judge serving under [the Act] shall have 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" certain duties, including among other things "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." *28 U.S.C. § 636(a)(1)*. *Federal Rule of Criminal Procedure 41(b)* provides in relevant part:

Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a

warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; . . .

(4) a magistrate judge **[*9]** 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 . . . .

The Court finds, and the Government seemingly concedes, that neither *Rule 41(b)(1)* nor *Rule 41(b)(2)* authorized an Eastern District of Virginia magistrate judge to issue the NIT

Warrant.5 Those two provisions authorize a magistrate to issue a warrant only when the property

to be searched is "located within the district" at the time the warrant issues. Here, only the

Playpen website-located on a Government server under FBI control-was located in the

Eastern District of Virginia. The very information the NIT Warrant was designed to uncover,

however-i.e., the IP addresses and other identifying information of Playpen users-was not

located in the Eastern District of Virginia. That information necessarily had to be retrieved from

the "activating computers," which in this case were both located in Iowa. Indeed, only once the

NIT was deployed onto Defendants' computers did their computers relay the information sought

by investigators back to the Playpen website. **[*10]** *See* NIT Warrant ¶ 33 (explaining that the NIT

would be deployed to an activating computer when a user logged into the Playpen website

whereafter "the instructions, which comprise the NIT, are designed to cause the user's

5 The Government's sole reference to the first two subsections of *Rule 41(b)* in its

resistance brief is as follows: "Defendants argue that the NIT search warrant fails to satisfy *Rule 41(b)(1)* and *(b)(2)* because some of the computers searched by the NIT warrant, including those of defendants, were not located in the Eastern District of Virginia, where the warrant was obtained, and that the server which hosted Website A, although located in the issuing district, was not where the search occurred." Gov't Resistance Br. at 4-5. The Government makes no argument, however, that

either (b)(1) or (b)(2) authorized issuance of the NIT Warrant. *See generally id*. Rather, it focuses solely on *Rule 41(b)(4)* in support of its assertion that the NIT Warrant was properly issued. *Id*. at 5-7.

'activating' computer to transmit certain information to a computer controlled by or known to the government"); ¶ 36 (explaining that the NIT would "attempt to cause the user's computer to send [certain information] to a computer controlled by or known **[*11]** to the government that is located in the Eastern District of Virginia"). Thus, the "activating computers," located outside of the Eastern District of Virginia, comprised the property to be searched pursuant to the NIT Warrant. Subsections (1) and *(2) of Rule 41(b)* are clearly inapplicable.

The Government urges that the NIT Warrant was permissible pursuant to *Rule 41(b)(4)*, because the Defendants "logged onto [Playpen] from computers located in the Southern District of Iowa, which triggered the NIT during the time period that the NIT tracking device was active, which gathered identifying information, including an IP address, for each of the defendant's computers." Gov't Resistance at 7. In support of its position, the Government cites *Matish* and

Darby. In *Matish*, the court found that Magistrate Judge Buchanan had authority to issue the NIT Warrant under *Rule 41(b)(4)* because Playpen users made "a virtual trip via the Internet to Virginia." 2016 WL 3545776, at *18. Thus, it concluded that the NIT "resembles a tracking device" in that the installation of the NIT occurred on "each individual computer that entered the Eastern District of Virginia when its user logged into Playpen via the Tor network. When that computer left Virginia-when the user logged out of Playpen-the NIT worked **[*12]** to determine its location, just as traditional tracking devices inform law enforcement of a target's location." *Id*. The *Darby* court likewise found the NIT Warrant permissible pursuant to *Rule 41(b)(4)*:

It is understandable why the government sought the warrant in the Eastern District of Virginia. The government planned to run the website from a server located in the district. No district in the country had a stronger connection to the proposed search than this district. Additionally, nothing in *Rule 41* categorically

forbids the magistrates from issuing warrants that authorize searches in other districts-most of its provisions do just that. . . .

Rule 41(b)(4) allows a magistrate judge to issue a warrant for a tracking device to be installed in the magistrate's district. Once installed, the 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 the district, sent information to the government **[*13]** about their location. The magistrate judge did not violate *Rule 41(b)* in issuing the NIT Warrant.

2016 WL 3189703, at *11-12.

The Court finds *Darby* and *Matish* unpersuasive. The Court additionally disagrees with

the *Jean* decision, which was decided after the Government filed its resistance brief. There, the

court found that the NIT 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." 2016 WL 4771096, at *16. The court reasoned:

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. In such instances, *Rule*

41(b)(4) allows a magistrate judge to authorize law enforcement's use of electronic tracking tools and techniques. 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 **[*14]** outside the Eastern District of Virginia-is not only authorized by *Rule 41(b)(4)*, but is the very purpose intended by the exception.

2016 WL 4771096, at *17.

A "tracking device" is defined for purposes of *Rule 41* as any "electronic or mechanical

device which permits the tracking of the movement of a person or object." *See Rule 41(a)(2)(E)*

(employing the definition of "tracking device" as set out in *18 U.S.C. § 3117(b)*). Although the

term "track" is not further defined, its ordinary meaning is "[t]o follow up the track or footsteps of; to trace the course or movements of; to pursue by or as by the track left." *See http://www.oed.com* (last visited Sept. 19, 2016). The NIT here at issue, however, clearly did not "track" the "movement of a person or object." Indeed, it did not "track" the "movement" of anything; rather, it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia. Thus, the plain language of *Rule 41* and the statutory definition of "tracking device" do not, in this Court's opinion, support so broad a reading as to encompass the mechanism of the NIT used in this case. *See Torres*, 2016 WL 4821223, at *6 (holding that it "is inappropriate for this Court to engage in a process of finesse **[*15]** justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of [*Rule 41(b)*] as now written does not provide jurisdiction under these circumstances"). The limitations of *Rule 41(b)(4)* and its inapplicability to the NIT Warrant issued in this case are further evidenced by the fact that absent Congressional intervention, *Rule 41* will be amended on December 1, 2016, to add subsection (b)(6), which provides in relevant part that "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 information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means." *See id.* (finding that "the existence of the proposed amendment indicates at a minimum that there is currently ambiguity as to the state of the law" and thus, "[b]olster[s]" the argument that *Rule 41(b)(4)* did not justify issuance of the NIT Warrant).

Having rejected the position advanced by the Government, the Court instead agrees with

the numerous district courts who have concluded that Magistrate Judge Buchanan lacked

authority to issue the NIT Warrant **[*16]** under *Rule 41(b)(4)*. In particular, the Court agrees with

Michaud, wherein the court found that application of *Rule 41(b)(4)* to the NIT Warrant

"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 [the out-of-state defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the out-of-state defendant's] computer, applying the tracking device exception again fails, because [the out-of state defendant's] computer was never physically located within the Eastern District

of Virginia.

2016 WL 337263, at *6; *see also Henderson*, 2016 WL 4549108, at *3 ("The NIT search does

not meet the requirements of 41(b)(4) because, even though it was analogous to a tracking

device in some ways, it nevertheless falls outside the meaning of a 'tracking device' as

contemplated by the rule. Further, the NIT was installed outside of the district, at the location of

the activating computers, not within the district as required by *Rule 41(b)(4)*."); *Werdene*, 2016

WL 3002376, at *7 (finding *Rule 41(b)(4)* inapplicable because it is "premised on the person or

property being located within the **[*17]** district" and because it is "uncontested that the computer

information that the NIT targeted was at all relevant times located beyond the boundaries of the

Eastern District of Virginia"); *Levin*, 2016 WL 2596010, at *6 (finding unpersuasive the

government's attempt to analogize the transmittal of the NIT to activating computers to "the

installation of a tracking device in a container holding contraband"); *Arterbury*, No. 15-cr-182,

Clerk's No. 42 at 17 (agreeing with *Michaud* and concluding that the "NIT warrant was not for

the purpose of installing a device that would permit authorities to track the movements of

Defendant or his property"). The Court thus concludes that Magistrate Judge Buchanan lacked authority to issue the NIT Warrant pursuant to any provision of *Rule 41(b)*.

B. *What is the Remedy for the Rule 41(b) Violation?*

"*Rule 41* and the *Fourth Amendment* are not coextensive," and "[n]oncompliance with *[Rule] 41* prerequisites does not automatically require the exclusion of evidence in a federal prosecution." *United States v. Schoenheit, 856 F.2d 74, 76-77 (8th Cir. 1988)*. "Absent a constitutional infirmity, the exclusionary rule is applied only to violations of Federal Rule 41 that prejudice a defendant or show reckless disregard of proper procedure." *United States v. Hyten, 5 F.3d 1154, 1157 (8th Cir. 1993)* (citing *United States v. Freeman, 897 F.2d 346, 348-49 (8th Cir. 1990)*); *see also United States v. Welch, 811 F.3d 275, 280-81 (8th Cir. 2016)* (stating that a defendant "must show, in addition to the Rule 41 violation, either **[*18]** that he was prejudiced by the violation or that the investigators recklessly disregarded proper procedure").

1. *Constitutional violation*.

Once a court determines that a Rule 41 violation has occurred, it must next "determin[e] whether that specific Rule 41 violation rises to the level of a *Fourth Amendment* violation."

United States v. Krueger, 809 F.3d 1109, 1113-14 (10th Cir. 2015). If it does, the violation can be considered constitutional and suppression is warranted without further evidence of prejudice or reckless disregard. *See id*. at 1114 ("Unless the defendant can establish prejudice or intentional disregard of the Rule, a non-constitutional violation of Rule 41 will not, by itself, justify suppression.").

Only the *Levin* and *Arterbury* courts have explicitly held that the *Rule 41(b)* violation in relation to issuance of the NIT Warrant was of constitutional concern. In *Levin*, the court

reasoned that *Rule 41(b)* violations cannot be considered merely ministerial or procedural because the Rule "involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant." 2016 WL 2596010, at *7 (citing *United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008)* (holding that *Rule 41(b)* "deals with substantive judicial authority-not procedure") and *Krueger, 809*

F.3d at 1115 n.7 (concluding that Rule 41(b)(1) is "unique from other provisions of Rule 41 because it implicates 'substantive judicial authority'")). **[*19]** Stated another way, because "the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval" of the NIT Warrant as required by the *Fourth Amendment*. *Id*. at *8. Accordingly, the *Levin* court held that the NIT Warrant was void *ab initio*, "akin to no warrant at all," and that suppression was necessary. *Id*. at *8, 12; *see also Arterbury*, No. 15-cr-182, Clerk's No. 42 at 26 (relying on

Krueger and*Levin* to conclude that "where the Rule 41 violation goes directly to the magistrate judge's fundamental authority to issue the warrant, as in the violation presented here, it is not a 'technical violation' of the Rule" and "suppression is warranted"). It further held that the *Leon* good faith exception could not save evidence gathered as a result of the NIT Warrant because the exception is inapplicable in cases where the warrant is void from the outset. *Levin*, 2016 WL 2596010, at *10-13 (alternatively holding that it would decline to apply the *Leon* exception even if it were applicable because it was "not objectively reasonable for law enforcement . . . to believe that the NIT was properly issued considering the plain mandate of *Rule 41(b)*" and because "the conduct at issue here can be described as 'systemic error or reckless disregard **[*20]** of constitutional requirements'" (quoting *Herring v. United States, 555 U.S. 135, 147 (2009)*); *see also Arterbury*, No. 15-cr-182, Clerk's No. 42 at 26 (agreeing with *Levin* that where the "warrant is void *ab initio*, suppression is warranted and the good-faith exception is inapplicable").

Upon careful review of the case law, this Court adopts the well-reasoned decisions in

Levin and*Arterbury* and concludes that a warrant issued without proper jurisdiction is void *ab initio* and that any search conducted pursuant to such warrant is the equivalent of a warrantless search. *See Levin*, 2016 WL 2596010, at *12; *Arterbury*, No. 15-cr-182, Clerk's No. 42 at 26; *see also United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013)* (rejecting the notion that violation of the jurisdictional limitations of *Rule 41(b)* is merely a "technical defect"); *United States v. Barber*, No. 15-40043, 2016 WL 1660534, at *3 (D. Kan. Apr. 27, 2016) (holding that "warrants issued without jurisdiction are void from their inception. A warrant that is void from its inception is not warrant at all." (citing *Krueger, 809 F.3d at 1124-25*)). "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley v. California, 134 S. Ct. 2473, 2482 (2014)*. Here, the Government does not argue that a warrantless search was permissible under the circumstances of this case.6 The warrantless search was, therefore, presumptively unreasonable and suppression is an appropriate **[*21]** remedy unless the *Leon* good faith exception applies.*7Kentucky v. King, 563 U.S. 452, 461*

6 In its argument that Defendants were not prejudiced by the *Rule 41(b)* violation, the Government urges that Defendants had no reasonable expectation of privacy in the IP addresses obtained by virtue of the NIT Warrant. Gov't Resistance Br. at 10-11. This argument could reasonably be construed as implying that no warrant was required to obtain Defendants' IP addresses, and thus, there could not have been a *Fourth Amendment* violation requiring suppression. *See Matish*, 2016 WL 3545776, at *18-24 (finding that no warrant was required to deploy the NIT because defendants have no reasonable expectation of privacy in either their IP addresses or in their computers). For reasons discussed *infra*, the Court rejects the proposition that Defendants lacked a reasonable expectation of privacy in the information obtained by virtue of the NIT Warrant under the circumstances of this case.

7 The Court fully recognizes that "[f]or exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Davis v. United States, 564 U.S. 229, 237 (2011)*. In this

case, the Court believes that the societal costs asserted by the Government (*see* Gov't Resistance Br. at 15) are outweighed by the fact that suppression will "deter[] police from **[*22]** obtaining warrants from judges who lack jurisdiction to issue them." *Barber*, 2016 WL

(2011) ("[W]e have often said that searches and seizures inside a home without a warrant are presumptively unreasonable." (quotation marks and citations omitted)). For the same reasons asserted in *Levin*, however, the Court finds that *Leon* is inapplicable to issuance of the NIT Warrant because the NIT Warrant was issued without jurisdiction and was, therefore, void *ab initio*. *Levin*, 2016 WL 2596010, at *11-13; *see also Barber*, 2016 WL 1660534, at *3 ("[T]he good faith exception applies only to evidence seized under a once-valid warrant that was subsequently invalidated-not evidence seized pursuant to a warrant that was void at its inception."). Moreover, because there would not have been probable cause to issue the Iowa Warrants without the information obtained from the NIT Warrant, all evidence seized as a result of the Iowa Warrants must be suppressed as fruit of the poisonous tree. *See* *Wong Sun v. United States, 371 U.S. 471, 487-88 (1963)*.

2. *Technical violation.*

Assuming that the *Rule 41(b)* violation was merely technical, the Court would still find suppression appropriate in this case for the reasons articulated in *Levin* and *Arterbury*. As discussed *supra*, if the *Rule 41(b)* violation is considered non-constitutional, suppression is only warranted **[*23]** if Defendants were prejudiced by the violation or if there is evidence that law enforcement recklessly disregarded procedure. *See* *Schoenheit, 856 F.2d at 76-77*. In the Eighth Circuit, prejudice may be found where "the search might not have occurred or would not have been so abrasive if the Rule had been followed," whereas reckless disregard may be found where "there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Freeman, 897 F.2d 346, 349-50 (8th Cir. 1990)* (quoting *United States v. Burke, 517 F.2d 377, 386-87 (2d Cir. 1975)* and *United States v. Luk, 859 F.2d 667, 671 (9th Cir. 1988)*).

1660534, at *4.

The Government cites *United States v. Wheelock* in support of its assertion that

Defendants could not have been prejudiced by the *Rule 41(b)* violation because they had no

reasonable expectation of privacy in the specific information obtained by the NIT Warrant, i.e.,

in their IP addresses and other identifying information obtained from their computers. *See* Gov't

Br. at 10 (citing *Wheelock, 772 F.3d 825 (8th Cir. 2014)*). In *Wheelock*, the Eighth Circuit

considered whether a defendant's *Fourth Amendment* rights were violated when law

enforcement obtained an administrative subpoena that directed the defendant's ISP to provide

subscriber information associated with a particular IP address:

Wheelock argues the use of an administrative subpoena (as opposed to a warrant) violated his *Fourth Amendment* privacy interest in the subscriber information obtained from Comcast. **[*24]** To prove he had a constitutionally cognizable privacy interest, Wheelock "must show that (1) he 'has a reasonable expectation of privacy in the areas searched or the items seized,' and (2) 'society is prepared to accept the expectation of privacy as objectively reasonable.'" *United States v. James, 534 F.3d 868, 872-73 (8th Cir. 2008)* (quoting *United States v. Hoey*, 983F.2d 890, 892 (8th Cir.1993)).

"'[T]he *Fourth Amendment* does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the

assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.'" *United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011)* (quoting *United States v. Miller, 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed.2d 71 (1976)*) . This principle is dispositive here. With Comcast in possession of his subscriber data, Wheelock cannot claim a reasonable "'expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.'" *Suing*, 712 F.3d at 1213 (alteration in original) (quoting *United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009)*); accord *United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008)* ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the *Fourth Amendment's* privacy expectation.").

*Wheelock, 772 F.3d at 828-29.*8As Defendants correctly point out in their briefs, *Wheelock* is plainly distinguishable. **[*25]** *See* Croghan Br. at 19. In *Wheelock*, law enforcement obtained the defendant's IP address *from the defendant's ISP*. Here, by contrast, law enforcement caused an NIT to be deployed directly onto Defendants' home computers, which then caused those computers to relay specific information stored on those computers to the Government without Defendants' consent or knowledge. There is a significant difference between obtaining an IP address *from a third party* and obtaining it *directly from a defendant's computer*. *See Riley, 134 S. Ct. at 2492-93* (finding a distinction between evidence about phone usage obtained from the phone company and evidence about phone usage obtained directly from the phone itself). If a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper-even accepting that the defendant had no reasonable expectation of privacy in the IP address itself. Here, Defendants' IP addresses were stored on their computers in their homes rather than in a drawer. Law enforcement has admitted, however, that it had no way to learn Defendants' IP addresses without deploying the NIT and essentially **[*26]** forcing Defendants' computers to relay identifying information to Virginia. While the IP addresses may have themselves been evidence of a crime, Defendants nonetheless had a reasonable expectation of privacy in the locations where the IP addresses were stored, necessitating that law enforcement obtain a valid warrant before searching such locations. *See, e.g.*, *United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008)* (recognizing that individuals generally have an objectively

8 The Government additionally cites *Michaud*, 2016 WL 337263, and *Matish*, 2016

WL 3545776, which both concluded that issuance of the NIT Warrant did not violate the *Fourth Amendment* because the defendants could not have had a reasonable expectation of privacy in their IP addresses.

reasonable expectation of privacy in their personal computers); *United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)* ("Individuals generally possess a reasonable expectation of privacy in their home computers."). This distinction supports the Court's conclusion that a valid warrant was required to obtain information directly from Defendants' home computers, even assuming the Defendants lacked an objectively reasonable expectation of privacy in the information actually gathered.

It is clear in this case that neither the search pursuant to the NIT Warrant nor the searches pursuant to the Iowa **[*27]** Warrants would have occurred without the violation of *Rule 41(b)*. Had Rule 41 been complied with, law enforcement would not have obtained Defendants' IP addresses, would not have been able to link those IP addresses to Defendants through subsequent investigation and the use of administrative subpoenas, and would not have had sufficient probable cause to obtain the Iowa Warrants. Thus, Defendants have satisfied their burden to prove that they were prejudiced by

the *Rule 41(b)* violation. Suppression is an appropriate means to deter law enforcement from seeking warrants from judges lacking jurisdiction to issue them, and this deterrence function outweighs the societal costs associated with suppression. Moreover, the Court finds that law enforcement was sufficiently experienced, and that there existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant, that the good faith exception is inapplicable. *See Levin*, 2016 WL 2596010, at *13 (finding that the good faith exception would be inapplicable even if the *Rule 41(b)* violation was not constitutional because the "conduct at issue here can be described as 'systemic error or reckless disregard of constitutional requirements'" and because "it was not objectively **[*28]** reasonable for law enforcement-particularly 'a veteran FBI agent with 19 years of federal law enforcement experience'-to believe the NIT Warrant was properly issued considering the plain mandate of *Rule 41(b)*" (citing *Glover, 736 F.3d at 516* ("[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'")); Croghan Br. at 20-21 (citing case law supporting a conclusion that law enforcement should have been aware that *Rule 41(b)* had jurisdictional limits that would prevent issuance of the NIT Warrant).

III. CONCLUSION

For the reasons stated herein, Defendants' Motions to Suppress (Croghan Clerk's No. 33; Horton Clerk's No. 45) are GRANTED. All evidence flowing from and obtained as a result of the improperly issued NIT Warrant is hereby suppressed.

IT IS SO ORDERED.

Dated this _19th__day of September, 2016.

End of Document