IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

No: 16-3976

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

STEVEN SHANE HORTON

Defendant-Appellee.

Appeal from the United States District Court for the
Southern District of Iowa – Council Bluffs

Honorable Robert W. Pratt

BRIEF OF APPELLEE

STUART J. DORNAN, #18553
Dornan, Lustgarten & Troia PC LLO
1403 Farnam Street, Suite 232
Omaha, NE 68102
(402) 884-7044
ATTORNEY FOR APPELLEE

SUMMARY OF THE CASE AND REQUEST FOR ORAL ARGUMENT

The Government has filed a consolidated appeal from an order of the district court suppressing evidence against Steven S. Horton and Beau B. Croghan. Law enforcement officers used a Network Investigative Technique Warrant obtained from a magistrate judge in the Eastern District of Virginia and obtained information from the State of Iowa.

Steven S. Horton suggests that fifteen minutes of oral argument would be sufficient.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES: Page Nos.

STATEMENT OF THE ISSUES

1. WHETHER THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT

    28 U.S.C. § 636(a)(1).

2. WHETHER SUPPRESSION WAS THE APPROPRIATE REMEDY IN THIS CASE

    United States v. Welch, 811 F.3d 275 (8th Cir. 2016).

    United States v. Spencer, 439 F.3d 905 (8th Cir. 2006).

STATEMENT OF THE CASE

A federal grand jury in the Southern District of Iowa returned an indictment against Appellee, Steven S. Horton, for accessing or attempting to access child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Horton filed a motion to suppress the evidence that was obtained as a result of a Network Investigative Technique Warrant ("NIT Warrant"). The facts for purposes of the motion to suppress were not in dispute. The District Court granted Horton's motion and suppressed all of the evidence that was obtained and flowed from the NIT Warrant. The Government filed an appeal that was consolidated with a companion case, United States of America v. Beau Brandon Croghan, 15-CR48 (S.D. Iowa).

STATEMENT OF FACTS

A child pornography investigation was initiated in 2014 by the Federal Bureau of Investigation ("FBI") into a website known as "Playpen." Affidavit in support of NIT Warrant, ¶ 11. Playpen was identified as a "hidden service" on the "Tor" network that contained child pornography and provided for user anonymity. *Id*. ¶ 10. Investigation led the FBI to be able to seize the Playpen website server. *Id*. ¶ 28. A copy was made of the website and placed onto a government-controlled served located in Newington, Virginia so that the FBI could attempt to identify users of the site while running it. *Id*.

On February 20, 2015, the FBI submitted an application for and affidavit in support of a search warrant to a Magistrate Judge in the Eastern District of Virginia. The application included a request to be authorized to use a Network Investigative Technique ("NIT") that would involve adding software to the government-controlled Playpen website that would assist in identifying the users. *Id*. ¶ 30. The software would deploy the NIT onto any computer that was used to enter a login and password to the Playpen website. *Id*. ¶ 31. The NIT would then transfer a great deal of identifying information back to the FBI from the computer including the internet protocol address ("IP address"). *Id*. ¶ 34. The warrant was granted, and the FBI used the NIT for approximately two weeks.

On August 5, 2015, approximately five months later, a search warrant was obtained for Steven Horton's residence in Glenwood, Iowa. The NIT that had been deployed from Virginia was responsible for the identifying information used to obtain the search warrant of Horton's residence in Iowa.

SUMMARY OF THE ARGUMENTS

Rule 41(b)(4) did not permit the NIT Warrant because the functions of the technique were substantially different than that of a tracking device. Authorization of a tracking device to track physical location is not the same thing as using a technique to collect identifying information well beyond that of a person or object's physical location.

Suppression of the evidence was the appropriate remedy because the Rule 41 violation rose to the level of a Fourth Amendment violation and both prejudice and a reckless disregard for procedure were present. The warrant was void *ab initio* and therefore it was as if a search was conducted without a warrant thereby establishing that a constitutional violation had occurred. In addition, prejudice occurred to Horton because had there not been a violation resulting in identifying information, the Iowa search warrant never would have been granted. Finally, suppression remains appropriate because it was not objectively reasonable for the law enforcement officers to believe the NIT Warrant was properly issued.

ARGUMENTS

I. THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT.

The Magistrate Judge lacked authority under Rule 41(b)(4) to issue the NIT Warrant because the FBI's technique in the NIT Warrant went beyond, or was otherwise substantially different from, what the plain language of the rule provided for. Even allowing for some flexibility in the interpretation of the rule does not make it into something that fits. Simply put, the technique deployed did not do what a tracking device does.

The NIT Warrant requested in the present case did not seek a tracking device. Rather, it sought authorization to probe (search) and collect (seize)

identifying information from computers in whatever jurisdiction they happened to be physically located in. 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:
>
> …
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both. . . .

Id. For purposes of Rule 41, a tracking device is defined as any "electronic or mechanical device which permits the tracking of the movement of a person or object." *See* Rule 41(a)(2)(E) (referencing 18 U.S.C. § 3117(b)). As amended December 1, 2016, Rule 41now includes subsection (b)(6) providing for:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Fed. R. Crim. P. 41(b)(6).

First, it is worth noting that the term "tracking device" is not found anywhere in subsection (6). What is found in subsection (6) is language that would

seem to fit what the NIT Warrant set out to do in the present case. The FBI was not interested in receiving just the longitude and latitude coordinates of the computer so that its physical location could be monitored as it changed coordinates and ended up in a different physical location than prior to the movement. Rather, the NIT Warrant wanted:

> a. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
>
> b. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;
>
> c. 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);
>
> d. Information about whether the NIT has already been delivered to the "activating" computer;
>
> e. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communications, such as communications over the Internet;
>
> f. [T]he "activating" computer's active operating system username; and
>
> g. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is

> intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

Affidavit in support of NIT Warrant, ¶ 34. Paragraphs 31 through 37 of the affidavit describe the Network Investigative Technique. An explanation is given including the above-itemized list of information to be collected. Nowhere in those paragraphs does the affidavit indicate that the technique intends to track the movement of a person or property. Paragraph 33 indicates that only "certain information" will be caused to be transmitted. Although the word "search" is not used, a search must be employed if information will be sorted through so that only "certain information" is transmitted. Paragraph 36 uses the language "attempt to cause the user's computer…" which is synonymous with "force" and "seize" in certain contexts.

Numerous courts have rejected the argument that the NIT was the equivalent of a "tracking device" under Rule 41(b)(4). Most critically, the installation of the NIT did not take place in the Eastern District of Virginia but in the district where the computer was physically located. *See United States v. Levin*, 2016 WL 2596010, at * 6, n. 9 (D. Mass. May 5, 2016); *United States* v. *Michaud*, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016); *see also In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) (rejecting government's application for a warrant to deploy software to remotely

extract identifying information from a computer in an unknown location, because "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.").

The Government cited *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994) for the position that it is better to interpret Rule 41 in such a manner as to not encourage law enforcement to resort to warrantless searches. (Government's brief at 20). This position argues for the extreme of an "overly flexible" interpretation to avoid the extreme of "too narrow" of an interpretation. Additionally, the Government focuses more on the fact that an electronic means was used versus focusing on the nature of the information that the NIT sought as compared to that of a tracking device. Accordingly, the District Court did not error in concluding that the Magistrate Judge lacked authority to issue the NIT Warrant under Rule 41(b)(4).

II. SUPPRESSION WAS THE APPROPRIATE REMEDY IN THIS CASE.

A Rule 41 violation amounts to a violation of the Fourth Amendment warranting exclusion only if a defendant is prejudiced or if a reckless disregard of proper procedure is evident. *United States v. Welch*, 811 F.3d 275, 279 (8th Cir. 2016) quoting *United States v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006).

The violation here is not a "technical" violation of Rule 41, but one that speaks to the substantive constitutional protections embodied in Rule 41. *See United States v. Williamson*, 439 F.3d 1125, 1133 (9th Cir. 2006) (distinguishing between Rule 41 violations that are "mere technical error" and those rising to a "constitutional magnitude"). The Seventh Circuit has explained that "Rule 41(b) deals with substantive judicial authority—not procedure." *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008).

In *United States v. Levin*, 2016 WL 2596010 (D. Mass. May 5, 2016), the District of Massachusetts found the Rule 41 violation triggered the substantive protections of the rule because the error involved "the authority of the magistrate judge to issue the warrant" rather than simply "the procedures for obtaining and issuing warrants." *Levin*, 2016 WL 2596010, at *7-8 (quoting *United States v. Krueger*, 809 F.3d 1109, 1115 n. 7 (10th Cir. 2015) (quotations omitted)). More specifically, the court found that because "the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval." *Levin*, 2016WL 2596010, at *8. Without jurisdiction to issue the warrant, it was simply "void." or void *ab initio*, "akin to no warrant at all." *Id; see also United States v. Arterbury*, No. 15-cr-182, Clerk's No. 42 (N.D. Okla. Apr. 25, 2016) (agreeing with *Levin* that where the "warrant is void *ab initio*, suppression is warranted and the good-faith exception is in applicable).

Other courts have reached similar results with respect to warrants that violated the jurisdictional limitations of Rule 41. In *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), the D.C. Circuit suppressed a Title III wiretap order that was issued in the District of D.C. but authorized the interception of communications in the District of Maryland and the Eastern District of Virginia. 736 F.3d at 510. The D.C. Circuit concluded that the wiretap violated both Title III and Rule 41(b), which it found "impose the same geographic limitations on warrants." *Id*. at 515. The warrant's failure to comply with Rule 41(b)'s geographic limitations was a "jurisdictional flaw" that could not be excused as a "technical defect" because the error was a "blatant disregard of a district judge's jurisdictional limitation." *Id*.

The District Court agreed with the reasoning in *Levin* and *Arterbury* and held 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. Without any exceptions to the warrant requirement being present and the presumption of the warrantless search being unreasonable, the District Court found that suppression would be appropriate unless the *Leon* good faith exception applies. *See Kentucky v. King*, 563 U.S. 452, 461 (2011); *Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (finding "warrant was so obviously deficient that we must regard the search as 'warrantless'"); *Coolidge v. New Hampshire*, 403 U.S. 443,

454-55 (1971) (The "most basic" Fourth Amendment rule is that warrantless searches "are per se unreasonable under the Fourth Amendment").

The Government argued that the NIT warrant met the 4th Amendment requirements of probable cause, particularization, and issuance by a neutral and detached magistrate. Inherent, however, in the requirement of a "magistrate" is authority. Without authority, the District Court's conclusion that the warrant was void *ab initio* was not in error. The Government seems to argue for severability of the warrant due to the "magistrate plainly ha[ving] authority…to issue the NIT Warrant…within her district." (Government's brief at 31). No authority was provided, however, for the position that severability would trump a void warrant.

A challenge for a technical violation of Rule 41 would still trigger suppression for the reasons that Horton was prejudiced and a reckless disregard of proper procedure is evident. Horton was prejudiced because the NIT Warrant, the August 2015 and later searches of his computers, as well as his statements to law enforcement after the search of his residence, would not have occurred if Rule 41(b) had been followed. Two other courts considering this same exact NIT warrant have found that defendants were prejudiced by the Rule 41 violation and suppressed the NIT warrant and subsequent search warrants obtained as a result of the NIT warrant. In *Levin*, *supra*, the District of Massachusetts found prejudice, finding that "the government might not have obtained the evidence it seized

pursuant to the residential warrant, [because] the application for that warrant was based on information it acquired through the execution of the NIT Warrant." *Levin*, 2016 WL 2596010, at *9 n. 16. Similarly, in *Arterbur*y, the Northern District of Oklahoma found prejudice because the defendant's computers would not have been searched had Rule 41(b) been followed because absent the government's deployment of the NIT, the physical location—IP address—of the computers accessing Playpen would not have been known. *Arterbury*, at 22. *Arterbury* relied on the Tenth Circuit's decision in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), which involved a computer believed to contain child pornography that was seized in the Western District of Oklahoma pursuant to a search warrant authorized by a magistrate judge in the District of Kansas. *Krueger* at 1111-12. The Tenth Circuit found that the Rule 41 violation prejudiced the defendant because but for the improper search warrant, the search ultimately would not have occurred. *Krueger* rejected the argument that "the Government may have been able to obtain a warrant from a federal magistrate judge" in the correct district, noting "such hypotheticals simply cannot cure the Government's gross negligence in failing to comply with Rule 41 in the first instance." *Id*. at 1117 (citing *Glover*, 736 F.3d at 514-15) (emphasis in original).

Here, there is no question that but for the Rule 41 violation, Horton's residence and computer would not have been searched. The entire basis of the

Southern District of Iowa search warrant was the evidence obtained from the NIT search warrant. It was the NIT that allowed the government to discover the IP address that the FBI investigated and tracked down to Horton's residence in Glenwood, Iowa. And, as a result of the Glenwood search warrant, the government obtained statements from Horton, seized computers and property belonging to Horton, and secured the present indictment and an additional search of Horton. The Government's position that a magistrate judge "surely would have authorized the very same searches of Horton['s] …computers that occurred." misses the point that there would have been no probable cause to believe anyone in the Magistrate's district was accessing the website to justify issuance of a district-wide search warrant.

The district court in *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan 28, 2016) analyzed this same exact NIT warrant. The District Court found a Rule 41 violation but determined there was no prejudice, believing since individuals have no Fourth Amendment expectation of privacy in their IP address, the government "eventually could have [] discovered" that information. *Michaud*, 2016 WL 337263, *7. But that is wrong for two reasons. First, to the extent the Ninth Circuit has found no expectation of privacy in an IP address, that was only with respect to an IP address the government attempted to obtain from a third party service provider, not information obtained from communicating with a user's

computer directly. *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) (finding no expectation of privacy when government installed pen register on Internet service provider's equipment at their facility).[1] Here, the NIT obtained the IP address from the "activating computers" directly and not by going to a third party service provider and seeking IP address information from the service provider's own facilities or records. There is no question that there is an expectation of privacy on the information stored on and generated by a person's computer and as a result, the Fourth Amendment applies. *See United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) ("as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer").

In *Riley v. California*, 134 S. Ct. 2473 (2014) the Supreme Court rejected the exact argument that the district court in *Michaud* relied upon. In *Riley*, the Court ruled that the Fourth Amendment's search incident to arrest exception to the Fourth Amendment warrant requirement did not extend to a cell phone found on an

---

[1] Several judges in the same district, in the context of historical cell site location information, have rejected the argument that an individual has no Fourth Amendment expectation of privacy in third party digital information that reveals a person's location. See, e.g., United States v. Williams, ___ F. Supp.3d ___, 2016 WL 492933, *3 (N.D. Cal. Feb. 9, 2016) (Orrick, D.J.); In re Telephone Information Needed for a Criminal Investigation, 119 F. Supp.3d 1011, 1020-26 (N.D. Cal. 2015) (Koh, D.J.); United States v. Cooper, 2015 WL 881578, *6-8 (N.D. Cal. Mar. 2, 2015) (Illston, S.D.J.).

arrestee's person at the time of their arrest. Before the Supreme Court, the government argued that police should be permitted to search incident to arrest a cell phone's call log consistent with *Smith v. Maryland*, 442 U.S. 735 (1979) which found no expectation of privacy in a person's dialing records. *Riley*, 134 S. Ct. at 2492. But the Supreme Court unanimously rejected that faulty analogy, noting that *Smith* only authorized the installation of a pen register on the phone company's equipment because that was not a "search" under the Fourth Amendment. Obtaining the same information from the phone directly—as opposed to obtaining it from the phone company—was indisputably a "search" protected by the Fourth Amendment. *Riley*, 134 S. Ct. at 2492-93.

Second, contrary to the district court's belief in *Michaud*, the IP address information was not available from other sources. The evidence as pointed out by the District Court in this case establishes that without the deployment of the NIT there would be no other way to view the information and use it to further the investigation. As a result, Horton has thus shown that he was prejudiced by the Rule 41 violation and suppression is therefore an appropriate remedy.

In addition to prejudice being shown, the evidence indicates that law enforcement officers demonstrated, at a minimum, a reckless disregard of proper procedure. *See United States v. Schoenheit*, 856 F.2d 74 (8th Cir. 1988); *United States v. Hyten*, 5 F.3d 1154 (8th Cir. 1993); *United States v. Freeman*, 897 F.2d

346 (8th Cir. 1990); *United States v. Welch*, 811 F.3d 275 (8th Cir. 2016). In the present case the District Court found 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." In *Levin*, *supra*, the district court found that the "conduct at issue here can be described as a 'systemic error or reckless disregard of constitutional requirements.'" *Id.*, 2016 WL 2596010, at *13. At the time the government applied for the NIT warrant in August 2015, several courts had ruled that a violation of Rule 41(b)'s territorial limitations could lead to suppression of evidence. The D.C. Circuit's decision in *Glover*, which suppressed a wiretap issued in one district and executed in another as a violation of Rule 41(b), was decided in 2013. *See Glover*, 736 F.3d at 514-15. Although the Tenth Circuit had not decided *Krueger* yet, the district court's opinion—which suppressed evidence seized from a warrant issued in Kansas but executed in Oklahoma—had been decided in February 2014. *See United States v. Krueger*, 998 F.Supp.2d 1032 (D. Kan. 2014).

Most pertinent here, at least one magistrate judge had expressed concerns about its authority to issue a similar warrant to deploy computer code as violating the territorial limits of Rule 41. In 2013, Magistrate Judge Stephen Smith of the Southern District of Texas issued an opinion rejecting the government's request for a search warrant that was remarkably similar to the NIT warrant. *See In re Warrant*

to Search a Target Computer at Premises Unknown, 958 F. Supp.2d 753 (S.D. Tex. 2013). The government sought a search warrant that would "surreptitiously install data extraction software on the Target Computer" which, once installed, "has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district." *In re Warrant*, 958 F. Supp.2d at 755. The government acknowledged that they did not know the location of the suspects or their computer. Judge Smith denied the warrant, noting that he had no authority under Rule 41(b) to issue a warrant because it was possible the computer would be outside of the Southern District of Texas. *Id*. at 756-58, 761.

Thus, in February 2015 the government was on notice that courts disapproved of the government violating the jurisdictional limitations of Rule 41. The fact that the government went ahead and sought out the NIT warrant anyway—particularly after the concerns articulated by Magistrate Judge Smith in 2013—demonstrates that its violation of Rule 41(b) was intentional and deliberate and warrants suppression.

Finally, the officers acted in intentional and deliberate disregard of Rule 41. Even where no prejudice occurs, suppression is appropriate where the government was not acting in good faith. *See United States v. Leon*, 468 U.S. 897, 922 (1984).

Particularly where the Government moved Website A's server from North Carolina to Virginia, there can be no credible argument that officers reasonably believed that none of the 214,898 members of Website A were located outside of Virginia. It is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located outside the authorizing district. In *In re Warrant*, the court stated that where the location of the target computer is unknown, "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." 958 F. Supp.2d at 757. It is unlikely that the Government was unaware of this opinion when it filed its application.

In any event, the Government was clearly aware that the NIT Warrant was not authorized when it made its application in February, 2015. A memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, introduces a proposed amendment to Rule 41(b) that would authorize the use of the NIT Warrant. *See* Reena Raggi, Report of the Advisory Committee on Criminal Rules, May 5, 2014, at 319.[2] Specifically, proposed Rule 41(b)(6) "would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the

[2]Available at: http://www.fpd- ohn.org/sites/default/files/Preliminary%20Draft%20of%20Proposed% 20Fed%20Rule%20Amendments%2015Aug2014.pdf.

district: (1) when a suspect has used technology to conceal the location of the media to be searched." Rebecca A. Womeldorft, Transmittal of Proposed Amendments to the Federal Rules, Oct. 9, 2015, at 8.[3] Where the memorandum introducing the proposal states that the change "had its origins in a letter from Acting Assistant Attorney General Mythili Raman," it is not feasible that the Government was unaware that such searches were not authorized under Rule 41(b). *See* Report of the Advisory Committee on Criminal Rules, at 324. Perhaps most telling, the memorandum states that the reason for the proposal is that the territorial venue provisions create "special difficulties" for the Government when investigating crimes involving electronic information. *Id*. at 325 (explaining that "a warrant for a remote access search when a computer's location is not known would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device."). The fact that the proposal requires an entirely new subsection to Rule 41(b), rather than a clarification to an existing subsection, demonstrates that there is no reasonable interpretation of any provision in Rule 41(b) that would permit such a search.

[3] Available at: http://www.uscourts.gov/file/18641/download.

The Government argues that suppression is not warranted because the officers were not "culpable for the magistrate judge's purported error." (Government's brief at 39). Case law was cited for instances where the error was made by a court clerk or the officers had a belief that the status of something was otherwise different. Here the officers had sufficient notice that this approach was, at a minimum, questionable. The District Court found as much holding that "law enforcement was sufficiently experienced, and that there was adequate case law casting doubt on magisterial authority to issue precisely this type of NIT warrant…" The Government seemingly argues that the law enforcement officers involved in this case have the capacity to develop a "sophisticated NIT" but should not be required to keep up on the developments with approval and disapproval of legal tactics that are challenged in the courts or amended in the rules. (Government's brief at 48). The Government's position is contrary to the facts of the case, and the District Court's findings were not it error.

Rule 41(b) provides explicit geographic limits on the magistrate judge's authority to issue search warrants and, under the circumstances presented here, precluded her from issuing a warrant authorizing the search of property outside the district. The rule is clear. It is not for this Court to rewrite it to keep up with new technological developments. It is for the United States Congress to address any

shortcomings in the Rule. Until that occurs, searches like the one in this case violate Rule 41(b) and must result in suppression.

In this case, the Rule 41(b) violations require suppression of not only the NIT warrant, but all other evidence "obtained as a product of illegal searches and seizures. *Wong Sun v. United States*, 371 U.S. 471, 484-88 (1963). That extends to evidence seized pursuant to a search warrant that was a "fruit" of the original illegal search. *Nardone v. United States*, 232 U.S. 383 (1914).

Here, the Glenwood search warrant—and the subsequent seizure and search of Horton's computer—as well as the statements Horton made to the law enforcement in August 2015 are the "fruit" of the illegal NIT warrant. Because the NIT warrant was invalid, all these fruits of that initial illegal search should remain suppressed as well.

CONCLUSION

For the foregoing reasons, Steven Horton respectfully requests that this affirm the District Court's Order suppressing all evidence seized as a result of the NIT Warrant.

Respectfully submitted,

Steven S. Horton, Appellee,

BY: /s/ Stuart J. Dornan
STUART J. DORNAN, #18553
Dornan, Lustgarten & Troia PC LLO
1403 Farnam Street, Ste. 232
Omaha, NE 68102
(402) 884-7044
ATTORNEY FOR APPELLEE

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

The brief complies with the type-volume limitation of Fed.R.App.P. 32(a)(7)(B) because it contains 4,668 words excluding the parts of the brief exempted by Fed.R.App.P. 32(a)(7)(C)(iii).

This brief complies with the typeface requirements of Fed.R.App.P. 32(a)(5) and 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman font, 14 point.

/s/ Stuart J. Dornan
Stuart J. Dornan, #18553
Attorney for Appellee

CERTIFICATE OF SUBMISSION AND VIRUS SCAN

I hereby certify that on this 27th day of December, 2016, I electronically submitted the APPELLEE BRIEF with the Clerk of the Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system after scanning it for viruses by using the Trend MicroOffice scan software program, which reported no viruses were found. Papers will be transmitted upon receipt of the Notice of Filing from the Clerk of Court.

/s/ Stuart J. Dornan
Stuart J. Dornan, #18553
Attorney for Appellee

CERTIFICATE OF SERVICE

I hereby certify that on December 27, 2016, I electronically filed the foregoing document with the Clerk of the District Court using the CM/ECF system which sent notification of such filing to the following:

Kevin E. VanderSchel, United States Attorney
Katherine McNamara, Assistant United States Attorney
Leslie R. Caldwell, Assistant Attorney General
Sung-Hee Suh, Deputy Assistant Attorney General
David B. Goodhand, United States Department of Justice

and I hereby certify that I have mailed by United States Postal Service the document to the following non CM/ECF participants:

Steven S. Horton, Appellee

/s/ Stuart J. Dornan
Stuart J. Dornan, #18553
Attorney for Appellee