No. _____

In The

Supreme Court of the United States

NEIL C. KIENAST & BRAMEN B. BROY,

Petitioners,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To The United States Court Of Appeals For The Seventh Circuit

PETITION FOR WRIT OF CERTIORARI

JOHN MILLER CARROLL LAW
JOHN MILLER CARROLL
226 South State Street
Appleton, WI 54911
(920) 734-4878
John@Jmclaw.net
Attorney for Petitioner Neil C. Kienast

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTIONS PRESENTED

This Court has applied the *U.S. v. Leon*, 468 U.S. 897 (1984) good faith exception in a variety of cases to include a knock and announce violation (*Hudson v. Michigan*, 547 U.S. 586, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)); an outdated arrest warrant (*Arizona v. Evans*, 514 U.S. 1, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995)); and a recalled warrant (*Herring v. United States*, 555 U.S. 135, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009)). Some of the circuit courts, including the Seventh Circuit in this case, are extending it to warrants that are deemed void *ab initio*. See also, *U.S. v. Levin*, 186 F. Supp. 3d 26 (1st Cir. 2017) and *U.S. v. Workman*, 863 F.3d 1313 (10th Cir. 2017). Can the good faith exception apply where there should have never been a warrant at all?

The questions presented are:

I. Does the *Leon* exception apply to the warrant in this case?

II. Was the multijurisdictional warrant valid?

III. Is there a valid privacy interest at stake that is subject to Fourth Amendment Protection?

IV. Is the governmental action of reproducing and distributing one of the largest collections of child porn so severe of misconduct that suppression is warranted?

LIST OF PARTIES

All parties appear in the caption of the case on the cover page.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES—Continued

Page

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

OPINIONS BELOW

The Eastern District of Wisconsin denied Petitioner Kienast's motion and held that the Network Investigative Technique ("NIT") was akin to a GPS tracking device, that there was no privacy interest in an IP address and in any case that the governmental misconduct in knocking on the wrong door to obtain The Warrant did not warrant suppression.

Concerning the same warrant and search, upon the motion of the Petitioner, the Central District of Illinois found The Warrant was issued in violation of Fed. R. Crim. P. 41(b) and was invalid *ab initio*. The Central District of Illinois also found the conduct of the Government to be afoul of the Joint-Petitioners' Fourth Amendment protections. Regardless the Central District of Illinois applied the *Leon* good faith exception in denying the Joint-Petitioners' motion for suppression of the evidence.

The Seventh Circuit similarly declined to address the validity of The Warrant and found the good faith exception to apply even where a warrant is void at inception.

JURISDICTION

This Court may exercise jurisdiction under 28 U.S.C. § 1254(1).

Jurisdiction is based on a Federal Question that has not, but should be, settled by this Court under Sup. Ct. R. 10(c).

This appeal raises issue with and is subject to interpretation of the Federal Rules of Criminal Procedure Rule 41 and 28 U.S.C. § 636(a) of the Federal Magistrates Act, which govern the issuance of an extraterritorial warrant in this case.

The Petitioners challenge the issuance of an extraterritorial warrant issued by a magistrate judge in the Eastern District authorizing the search via NIT exploit of many citizens outside the territory of the Magistrates own jurisdiction.

Finally, the Petitioners contend that in denying the Petitioners' motion to compel discovery and produce Agent Douglas McFarland for questioning and failing to disclose the method by which the search was conducted, violated the Defendants' right to a fair trial and confrontation rights as granted by the United States Constitution.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Petition for a Writ of Certiorari involves the Fourth Amendment right to be free from unreasonable searches and seizures and the Sixth Amendment right to trial by impartial jury of the state and district where

the crime shall have been committed as previously ascertained by law:

U.S. Const. amend. IV:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. VI:

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and District wherein the crime shall have been committed, which District shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Statutory Provisions

28 U.S.C. § 636(a) of the Federal Magistrates Act

STATEMENT OF THE CASE

While investigating a source of child porn in Naples Florida, the FBI by means of an unlawfully issued defunct warrant, the reproduction of many contraband

images and hosting of a server containing child pornography used to distribute the same, conducted an electronic search from a remote jurisdiction on thousands of American citizens.

With one broad sweeping motion, the NIT warrant in Operation Playpen was issued by a magistrate judge in the Eastern District. The Warrant authorized the electronic reproduction and distribution of child porn and for the FBI's entry and modification of thousands of personal computers. Thousands of people's computers were searched for a broad range of suspected contraband remotely via security exploit.

The magistrate did not have jurisdiction to issue such a vast warrant. The agents that applied for The Warrant excluded material information from its application and The Warrant itself is invalid. The Petitioners challenge the application of the good faith exclusion in such a scenario.

The District and Circuit Court denied the Petitioners' motions for suppression applying the *Leon* good faith exception while ignoring arguments concerning the knowledge of the agents who applied for The Warrant, why The Warrant was sought from a magistrate rather than Judge and the failure of the District Court to allow a hearing concerning the application process or any inquiry into the knowledge of the agent applying for The Warrant.

The Petitioners' contest that the search was unlawful and that in failing to disclose the source code and method by which the operation was executed the

defendants' rights against unreasonable searches and seizures, due process and confrontation have all been violated.

REASONS REVIEW IS NECESSARY

1. As of now there is a vast array of findings concerning the validity of The Warrant, the application of Rule 41, the privacy interest at stake and whether or not the Defendant has a right to a *Franks* hearing based on this affidavit and search.

CASES FROM SEVENTH CIRCUIT ADDRESSING ISSUE:

U.S. v. Epich, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (adopting magistrate judge's report and recommendation).

U.S. v. Owens, No. 16-CR-38-JPS, 2016 WL 7053195 (E.D. Wis. Dec. 5, 2016) (adopting magistrate judge's report and recommendation)

CASES FROM OTHER JURISDICTIONS ADDRESSING ISSUE:

Twelve courts have found that The Warrant did not violate § 636(a) of the Federal Magistrates Act and/or Rule 41 of the Federal Rules of Criminal Procedure. *U.S. v. Jones*, No. 3:16-cr-026, 2017 WL 511883 (S.D. Ohio Feb. 2, 2017); *U.S. v. Austin*, No. 3:16-cr-00068, 2017 WL 496374 (M.D. Tenn. Feb. 2, 2017); *U.S.*

v. Bee, No. 16-00002-01-CR-W-GAF, 2017 WL 424889 (W.D. Mo. Jan. 31, 2017) (adopting magistrate judge's report and recommendation); *U.S. v. Sullivan*, No. 1:16-cr-270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); *U.S. v. Dzwonczyk*, No. 4:16-CR-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. McLamb*, No. 2:16-cr-92, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); *U.S. v. Lough*, No. 1:16-CR-18, 2016 WL 6834003 (N.D. W. Va. Nov. 18, 2016); *U.S. v. Johnson*, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016) (adopting in part magistrate judge's report and recommendation); *U.S. v. Smith*, No. 4:15-CR-00467 (S.D. Tex. Sept. 28, 2016); *U.S. v. Jean*, 207 F. Supp. 3d 920 (W.D. Ark. 2016); *U.S. v. Eure*, No. 2:16-cr-43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *U.S. v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); *U.S. v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016); cf. *U.S. v. Laurita*, No. 8:13-CR-107, 2016 WL 4179365 (D. Neb. Aug. 5, 2016) (adopting magistrate judge's report and recommendation) (finding no violation of the statute or Rule by a NIT warrant issued in a different pornography website investigation).

Twenty-two District Courts have found that The Warrant did violate § 636(a) and/or Rule 41(b), but that the violation did not warrant suppression. *U.S. v. Gaver*, 3:16-cr-88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017); *U.S. v. Perdue*, No. 3:16-CR-305-D(1), 2017 WL 661378 (N.D. Tex. Feb. 17, 2017); *U.S. v. Pawlak*, No. 3:16-CR-306-D(1), 2017 WL 661371 (N.D. Tex. Feb. 17, 2017); *U.S. v. Kahler*, No. 16-cr-20551, 2017 WL

586707 (E.D. Mich. Feb. 14, 2017); *U.S. v. Deichert*, No. 5:16-CR-201-FL-1, 2017 WL 398370 (E.D.N.C. Jan. 28, 2017); *U.S. v. Vortman*, No. 16-cr-00210-THE-1, 2016 WL 7324987 (N.D. Cal. Dec. 16, 2016); *U.S. v. Hammond*, No. 16-cr-00102-JD-1, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *U.S. v. Duncan*, No. 3:15-cr-00414-JO, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *U.S. v. Stepus*, No. 15-30028-MGM, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *U.S. v. Scarbrough*, No. 3:16-CR-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. Allain*, No. 15-cr-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *U.S. v. Broy*, 209 F. Supp. 3d 1045 (C.D. Ill. 2016); *U.S. v. Knowles*, 207 F. Supp. 3d 585 (D.S.C. 2016); *U.S. v. Ammons*, 207 F. Supp. 3d 732 (W.D. Ky. 2016); *U.S. v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); *U.S. v. Henderson*, No. 15-cr-00565-WHO-1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *U.S. v. Adams*, No. 6:16-cr-11-Orl-40-GJK, 2016 WL 4212079 (M.D. Fla. Aug. 8, 2016); *U.S. v. Rivera*, No. 2:15-cr-00266-CJB-KWR (E.D. La. July 20, 2016); *U.S. v. Werdene*, 188 F. Supp. 3d 431 (E.D. Pa. 2016); *U.S. v. Stamper*, No. 1:15-cr-109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *U.S. v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

A few courts have declined to decide whether the statute and/or the Rule authorized The Warrant but found that exclusion was unwarranted regardless. *U.S. v. Schuster*, No. 1:16-cr-51, 2017 WL 1154088 (S.D. Ohio Mar. 28, 2017); *U.S. v. Tran*, No. 16-10010-PBS,

2017 WL 7468006 (D. Mass. Dec. 28, 2016); *U.S. v. Anzalone*, No. 15-10347-PBS, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); *U.S. v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016).

Four courts have suppressed the evidence. *U.S. v. Croghan*, 209 F. Supp. 3d 1080 (S.D. Iowa 2016); *U.S. v. Workman*, 205 F. Supp. 3d 1256 (D. Colo. 2016); *U.S. v. Arterbury*, No. 15-CR-182-JHP (N.D. Okla. May 17, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016).

2. The Courts have largely declined defendants an opportunity to conduct a Franks hearing concerning this search. The Petitioners suggest that further due process concerns are sure to arise with the issuance of warrants from completely different regions of the country.

The availability and practicality of subpoenaing an agent from another state to a hearing alone serves as a large hurdle to defendants in challenging multijurisdictional warrants.

The evolving law of issuing multijurisdictional warrants, the due process concerns, Fourth Amendment concerns and technological concerns all require the clarification of this Court.

As technology has evolved so have the complexities of a warrant's reach in the electronic world. Concerning this search alone courts have made many

inconsistent findings that range all the way from finding that there was no privacy interest in an IP address to suppressing evidence due to Fourth Amendment violations.

With the execution of the NIT warrant, did the Petitioners digitally reach into the state of the issuing magistrate? Or, did the NIT through accessing the registry of the various computers throughout the US reach into their homes and personal computers? Further clarification is needed regarding the issuance of such warrants and what must be considered by a Judge when issuing a warrant of this complexity and magnitude.

This Court's review would eliminate many hearings and additional opinions further splintering the findings of the Districts and Circuits below.

3. Review of this Court is necessary to clarify when governmental officials that are involved in mass scale crimes may use information they obtain as a result.

4. Warrants void *ab initio* are not subject to the *Leon* good faith exception.

With The Warrant being void *ab initio* it is as if no warrant was issued from the inception. It would follow that a warrantless search, when one was required, was per se unreasonable. One cannot act in objective good faith reliance on something that does not exist. See *U.S. v. Krueger*, 809 F.3d 109 (10th Cir. 2015) (Gorsuch,

J., concurring). Additionally, the four "per se" situations outlined in *Leon* triggering the exclusionary rule do not all contain a focus on law enforcement. A magistrate wholly abandoning his or her judicial role is one of those per se situations. See *U.S. v. Decker*, 956 F.2d 773 (8th Cir. 1992). While this Court has applied the *Leon* good faith exception in a variety of cases to include a knock and announce violation, an outdated arrest warrant and a recalled warrant, it has not been applied to a warrant void *ab initio*. Some of the circuit courts, including the Seventh and Eighth and First Circuits and others, have extended *Leon*'s application to warrants that are deemed void *ab initio*. See also, *U.S. v. Levin*, 186 F. Supp. 3d 26 (1st Cir. 2017) and *U.S. v. Workman*, 863 F.3d 1313 (10th Cir. 2017).

5. Incorrect analysis and application of the *Leon* exception and errors in finding of fact which lead to different conclusions throughout the United States pertaining to this search require superior court review.

The Seventh Circuit agreed with the Eighth and Sixth Circuits in concluding that this Court adopted a balancing test by requiring that in order for a court to suppress evidence it must find that the benefits of deterrence must outweigh the costs. See *U.S. v. Master*, 614 F.3d 236 (6th Cir. 2010).

The balancing test adopted originally by the Eighth Circuit looked at a presumption of applicability if no bad faith, a narrow review of the deterrence potential, and an overly weighted consideration of

"letting guilty and possibly dangerous defendants go[ing] free."

In this Court's 5-4 decision in *Herring v. United States*, 555 U.S. 135, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009), this Court considered the actions of all of the officers involved and found negligence as opposed to deliberate or reckless conduct, which was emphasized as crucial to the holding in the case. *Herring* at 140. To the extent *Herring* established a balancing test to guide future courts, the one applied in the panel's decision did not comport. The Eighth and Seventh Circuits held that *Leon* should apply. *U.S. v. Horton*, 863 F.3d 104, 1051 (8th Cir. 2017). Most notably, the Eighth Circuit found that there was no need to deter law enforcement from seeking similar warrants because the rule had been updated to allow for the same. *Id.*

When Petitioner Kienast requested information pertaining to the prior knowledge of the agents who applied for The Warrant at issue and inquired how the source code was written to operate the exploit the requests fell on flat ears.

The questions remain unanswered: What did the agents applying for The Warrant know and intend? How does the NIT source code execute? Does it require a human operator to select search functions?

The District Court in this matter indicated that no hearing with the affiant was necessary and proceeded with a hearing concerning merely the local agent who relied upon The Warrant.

The District Court subsequently made findings that there was no privacy interest in an IP address, a clear misunderstanding of the interests at stake and how the technology actually works.

Law enforcement officers demonstrated, at a minimum, a reckless disregard of proper procedure. As pointed out in *Horton*, 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 *U.S. v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), 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 *U.S. 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 *U.S. 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. 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. 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 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. 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.

6. The NIT Warrant did not seek attachment of a tracking device and the District erred in finding that it was akin to one. Rather, the NIT sought authorization to probe (search) and collect (seize) identifying information from computers in whatever jurisdiction they happened to be physically located in. The District Court erred in finding this malware to be akin to a GPS. Many courts have made this error and superior court review can clarify the state of the law in this country.

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 sought much more. Nowhere in the descriptive paragraphs did the affidavit indicate that the technique intended to track the movement of a person or property. Accordingly, it was not a tracking device and there was no authority under Rule 41(b)(4) to issue

the NIT Warrant, this is clear error contained within the opinions of the many District Courts.

Here, there is no question that but for the Rule 41 violation, the Petitioners' residences and computers would not have been searched. The entire basis of the subsequent 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 the Petitioners' residences as a result, the government obtained statements from the Petitioners, seized computers and property belonging to them and secured the present indictments.

There would have been no probable cause to believe anyone in the Seventh Circuit's jurisdiction was accessing the website to justify issuance of a Circuit-wide search warrant.

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. In *Riley v. California*, 134 S.Ct. 2473 (2014) this 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 arrestee's person at the time of their arrest. Before this 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. But this 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. It was held 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. Second, the IP address information was not available from other sources.

The Petitioners have shown that they were prejudiced by the Rule 41 violation and suppression is therefore an appropriate remedy.

The Government argues that suppression is not warranted because the officers were not culpable for the magistrate judge's purported error and that regardless the officers acted in "good faith." Here the officers had sufficient notice that this approach was, at a minimum, questionable.

The District Court in *Horton* 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. . . ."

CONCLUSION

Throughout the NIT cases the Government seemingly argues that the law enforcement officers involved in this search had the capacity to develop a "sophisticated NIT" which by its very nature executes preprogrammed computer code that uses an engineered browser exploit to circumvent personal computer security and discover personal information from a computers registry before modifying the code of the computer to rely information directly to the FBI, 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.

The Government's position is contrary to the facts of the case, and the District Court's findings were clear error. 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).

WHEREFORE, Petitioners respectfully request that this Court grant this Petition for a Writ of Certiorari.

Respectfully submitted,

JOHN MILLER CARROLL LAW
JOHN MILLER CARROLL
226 South State Street
Appleton, WI 54911
(920) 734-4878
John@Jmclaw.net
Attorney for Petitioner
Neil C. Kienast