Journal of Business & Technology Law

Volume 13 | Issue 1 Article 7

Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found

Kurt C. Widenhouse

KURT C. WIDENHOUSE*

Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found

INTRODUCTION

After receiving a tip in February 2015, the FBI took control of a child pornography website named "Playpen" – a site only accessible via the "dark web."[1] Rather than shutting down Playpen, the FBI apprehended the domain owner and operated the website from a government facility in the Eastern District of Virginia for two weeks in order to identify website users – those who were likely to download child pornography.[2] During that time, on February 20, 2015, a FBI special agent applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use a Network Investigative Technique, or "NIT,"[3] to investigate Playpen's users and administrators.[4] In support of the warrant application, the applying agent submitted a thirty-three page affidavit that set forth his basis for probable cause that deploying the NIT would uncover evidence of child exploitation crimes.[5]

* Kurt Widenhouse is a 2018 J.D. candidate at the University of Maryland Francis King Carey School of Law. The author would like to express gratitude to his friends, teachers, and family. Most of all, he would like to thank his mother, the kindest woman and best author he knows.

1. *In re* Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) [hereinafter NIT Warrant Affidavit]; *see infra* Part I.1.A (discussing technical explanation of TOR and the dark web).

2. Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE: CYBERSECURITY (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques.

3. "NIT," or "Network Investigative Technique," is a program used by the FBI to circumvent electronic concealment via TOR, *see* Part I.A.1, or Virtual Proxy Network (VPN). Although the exact details of how the exploit works have not been officially revealed to prevent its effectiveness from being compromised, it is generally understood that the NIT plants a program on the suspect's computer, which, when activated, reveals specific information about the computer to the FBI. This information includes the suspect's IP address.

4. *See* NIT Warrant Affidavit, *supra* note 1.

5. United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7053195, at *1–2 (E.D. Wis. Dec. 5, 2016).

Along with monitoring the site's normal content, the NIT sent additional instructions to a user's computer (referred to as the activating computer).[6] These extra instructions, when downloaded, would cause the activating computer to transmit certain information to a government computer located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether or not the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address.[7] The NIT would be deployed each time a user logged onto the, now government-controlled, website.[8] In the time following the issuance of the NIT warrant, the FBI obtained over 1,000 IP addresses from users logging into Playpen.[9] This unprecedented sting resulted in over 100 persons criminally charged with possession of child pornography.[10]

While the Playpen operation was a significant law enforcement success, with unquestionable social benefits, the NIT warrant and resulting onslaught of cases highlight the legal uncertainty of what constitutes a search in the electronic age. In dealing with the NIT warrant, circuits have disagreed on: (1) whether the NIT-issuing magistrate had authority to issue the warrants for a "search" outside his jurisdiction, (2) whether the FBI needed a warrant at all, and (3) what the appropriate remedy would be.[11]

As the precedent lies, it is disturbingly unlikely that the FBI's implementation of the NIT constitutes a search. For privacy proponents, there remains a ray of hope. While circuit courts have disagreed on a magistrate's authority to issue warrants for these electronic "searches," an amendment to Federal Rule of Criminal Procedure 41(b) has settled the issue by explicitly allowing warrants where the jurisdiction of the person or place to be searched has been concealed through electronic means.[12] Thus, it is possible that information collected by the FBI that did not previously require a warrant, now needs one. There is a new, specific, Federal Rule of Criminal Procedure allowing magistrates to issue such warrants. The real question is how the courts will view a warrantless deployment of the NIT. Because there is now a rule almost specifically tailored to NIT deployment, it is possible courts will be more likely to find NIT deployment is a search requiring such a warrant.

6. NIT Warrant Affidavit, *supra* note 1, ¶ 33.

7. *Id.* ¶¶ 33–34, 36.

8. *Id.* ¶ 36.

9. *The Playpen Cases: Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened

10. *Id.*

11. *See infra* notes 31, 33 and accompanying text.

12. *See* FED. R. CRIM. P. 41(b)(6).

I. TECHNICAL BACKGROUND, LEGAL BACKGROUND, AND NOTABLE CASES

It is necessary to lay a short technical foundation in order to understand how the law functions regarding electronic searches. For the purposes of this article, I will briefly explain what The Onion Router is and what IP addresses are. After the background, I will discuss the driving legal principles themselves, including Federal Rule of Criminal Procedure 41(b) and amendment thereof, the Fourth Amendment expectation of privacy and trespass as a test for the warrant requirement, suppression as a remedy, and the Good Faith Exception for law enforcement. Lastly, I will give examples how the circuit courts have applied the legal principles to The Onion Router and Internet Protocol addresses, resulting in a splintering of decisions.

A. Technical Background

1. What Is "TOR?"

The United States Naval Research Lab initiated The Onion Router ("TOR") in the 1990s as a means to protect government communications.[13] After acquiring independent sponsors,[14] TOR became an independent non-profit, available to the general public. Anyone can use TOR for legitimate reasons to "improve their privacy and security on the Internet,"[15] though the program is notorious for its more nefarious uses (i.e. child pornography and the "Silk Road"– a network for online drug purchases).[16] TOR operates via a group of volunteer-operated servers to create a network of "virtual tunnels," allowing users to connect to a website anonymously.[17] Rather than making a direct connection between a computer and a website, TOR routes a connection through different "nodes" in the TOR network, thereby obscuring aspects of how and where its users are accessing the Internet.[18] This allows users to circumvent software designed to censor content, to avoid tracking of their browsing behaviors, and to facilitate other forms of anonymous communication.[19] TOR also allows access to the "dark web," that is, those sites not indexed by search engines and which require specific software to access.[20] Playpen, for example, was only

13. *Inception*, TOR, https://www.torproject.org/about/torusers.html.en (last visited Dec. 1, 2017).

14. *Sponsors*, TOR, https://www.torproject.org/about/sponsors.html.en (last visited Dec. 1, 2017).

15. *TOR: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Dec. 1, 2017).

16. Nate Anderson & Cyrus Farivar, *How the feds took down the Dread Pirate Roberts*, Arstechnica, (Oct. 3, 2013, 12:00 AM), https://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/.

17. *Id.*

18. *Id.*

19. *Id.*

20. *See* Andy Greenberg, *Hacker Lexicon: What Is The Dark Web?*, WIRED, (Nov. 19, 2014, 7:15 AM), http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

available on the "dark web" and accessible via TOR, like many other clandestine websites.[21]

2. What Exactly Is an IP Address?

An Internet Protocol (IP) address is a "unique numerical address identifying each computer on the internet."[22] Every computer or server connected to the Internet has a unique IP address.[23] IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet.[24] IP addresses may also be static, if an ISP assigns a user's computer a specific IP address each time that computer accesses the Internet.[25] Computer servers, including web servers, use IP addresses to communicate with other computers.[26] In some sense, an IP address is like a physical address a carrier needs to direct a package. Computers use IP addresses to route and deliver "packets" of information to each other.[27] Just as a physical address tells mail carriers where to direct a letter, an IP address tells providers where a device is and how to find it. This method makes sending and receiving information over the internet possible.[28]

B. Legal Background

1. Rule 41 and Jurisdiction

Federal Rule of Criminal Procedure 41(b) originally described five scenarios in which a federal magistrate judge has authority to issue a warrant. Subsection (b)(1) states the general rule that, "a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located in the district."[29] The following four subsections provide that a magistrate judge has authority to issue a warrant: (2) if the person or property is located within the district but might move or be moved outside the district before the warrant is executed; (3) if the magistrate judge sits in a district in which activities related to terrorism have

21. *Id.*

22. *In re* Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 48 (D. Mass. 2005).

23. United States v. Forrester, 512 F.3d 500, 510 n.5 (9th Cir. 2007).

24. *See generally* Stephanie Crawford, *What is an IP address?*, HOW STUFF WORKS, http://computer.howstuffworks.com/internet/basics/question549.htm (last visited Dec. 1, 2017).

25. *Id.*

26. Affidavit In Support of Application For Search Warrant, In the Matter of the Search of Computers That Access Websites 1-23, ¶5(m), 13-1744 WC (July 22, 2013).

27. Crawford, *supra* note 24.

28. *Id.*

29. FED. R. CRIM. P. 41(b)(1).

occurred; (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat.[30]

Circuit courts are split over whether or not the magistrate judge in Virginia had authority under Rule 41(b)(1-5) to issue a warrant out of his jurisdiction regarding use of the NIT.[31] The most commonly cited justifications allowing such warrants were subsections (1), (2), and (4) – issuing a warrant for a search inside the district, a search for a person or property that started inside the district and moved out, and installing a tracking device while inside the district, respectively.[32] Even courts that found a magistrate lacked such authority usually did not agree that suppression is

30. FED. R. CRIM. P. 41(b)(2)–(5).

31. *See* United States v. Croghan, 209 F. Supp. 3d 1080, 1085–86 (S.D. Iowa Sept. 19, 2016), *rev'd and rem'd by* United States v. Horton 863 F.3d 1041 (July 24, 2017). A few district courts conclude that the NIT Warrant was unlawfully issued and suppressed all fruits of it. *See*, *e.g.*, United States v. Levin, 186 F. Supp. 3d 26, 35 (D. Mass. 2016); United States v. Workman, 205 F. Supp. 3d 1256, 1263 (D. Colo. 2016), *rev'd by* United States v. Workman 863 F.3d 1313 (2017). Other courts 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 United States v. Leon, 468 U.S. 897 (1984) good faith exception. *See, e.g.*, United States v. Torres, No. 5:16–cr–285, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); United States v. Adams, No. 6:16–cr–11, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); United States v. Acevedo–Lemus, No. 15–00137, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); United States v. Werdene, 188 F. Supp. 3d 431 (E.D. Pa. 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 other courts conclude that a magistrate possessed adequate authority to issue the NIT Warrant under Rule 41 such that there was no legal violation that would require suppression. *See*, *e.g.*, United States v. Jean, 207 F. Supp. 3d 920 (W.D. Ark. 2016); United States v. Eure, No 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016); United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016) (foregoing R. 41(b) jurisdictional analysis because the court was sitting Virginia, the issuing district); United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016); United States v. Austin, 230 F. Supp. 3d 828, (M.D. Tenn. 2017); United States v. Lough, 221 F. Supp. 3d 770, (N.D. W. Va., 2016); United States v. McLamb, 220 F. Supp. 3d 663 (E.D. Va. 2016); United States v. Sullivan, 229 F. Supp. 3d 647 (N.D. Ohio 2017).

32. *See supra* note 31 and accompanying text.

appropriate.[33] However, the recent change to the Federal Rules of Criminal Procedure renders this question moot.[34]

As of December 1, 2016, Rule 41 added a new provision to 41(b), amending magistrate power to issue search warrants outside their jurisdiction in certain circumstances.[35] The amendment reads:

> Federal Rule of Criminal Procedure 41(b)
>
> * * * *
>
> (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. . .*[36]
>
> * * * *

Thus, the Supreme Court approved a new provision,[37] now in effect, that resolves the question as to whether or not jurisdictional issues will prevent a magistrate from allowing use of the NIT to "search" outside their district.[38] The answer, taken from

33. *Leon*, 468 U.S. at 920 (explaining the requirements for the Good Faith Exception); *see Torres*, 2016 WL 4821223, at *6; *Adams*, 2016 WL 4212079, at *2; *Acevedo–Lemus*, 2016 WL 4208436, at *3; *Werdene*, 188 F. Supp. 3d at 436; *compare Michaud*, 2016 WL 337263, at *6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), and *Epich*, 2016 WL 953269, at *2 (rejecting Defendant's contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 186 F. Supp. 3d at 35 (finding suppression warranted because Rule 41 "implicates substantive judicial authority," Defendant was prejudiced even if the violation was technical, and the Good Faith Exception to the exclusionary rule is not available because the warrant was void *ab initio*).

34. As the case law stands, note that a majority of courts have refused to suppress evidence in these cases, regardless a finding that deployment of the NIT was a search and the magistrate lacked jurisdiction. To these courts, the Good Faith exception reigns supreme.

35. *Rule 41 Changes Ensure a Judge May Consider Warrants For Certain Remote Searches*, THE UNITED STATES DEPARTMENT OF JUSTICE ARCHIVES (June 20, 2016) https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

36. FED. R. CRIM. P. 41(b) (2016) (Emphasis added)

37. Pursuant to the Rules Enabling Act, the Supreme Court Propagates the Rules of Criminal Procedure, subject to Congressional Approval. *See* Rules Enabling Act, 28 U.S.C. § 2072 (1990).

38. The Advisory Committee's records, which highlight the reasoning the for the change, note:

> The proposal speaks to two increasingly common situations affected by the territorial restriction, each involving remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet. In the first situation, the warrant sufficiently describes the computer to be searched, but the district within

the plain text of the amendment, is clear that magistrate judges have such authority. However, the question whether deployment of the NIT is a search under the Fourth Amendment remains unanswered.

2. Fourth Amendment and Expectation of Privacy

While Rule 41 deals with a magistrate's jurisdiction for warrants, the warrant requirement itself protects U.S. persons from unreasonable government intrusion. Law enforcement does not need a warrant if no "search" occurs.[39] "Searches" only require warrants when a government actor implicates the Fourth Amendment.[40] The Supreme Court of the United States has "uniformly . . . held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by the government action."[41] That inquiry is analyzed in two parts: (1) whether the individual, through his conduct, "exhibited an actual (subjective) expectation of privacy;" and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable'" (i.e. an objective expectation of privacy).[42]

i. Subjective Expectation of Privacy

To meet a subjective expectation of privacy, one must demonstrate that he had an actual, personal expectation of privacy.[43] In other words, a person asserting the government conducted a search requiring a warrant must show that he held the evidence in a manner designed to ensure its privacy.[44] Thus, while the Court in *Katz v. United States* and *Smith v. Maryland* extended Fourth Amendment protection to what a person goes to lengths to keep private, the Court did not protect activities one

> which the computer is located is unknown. This situation is occurring with increasing frequency *because persons who commit crimes using the Internet are using sophisticated anonymizing technologies . . . [such as] proxy services designed to hide their true IP addresses*.

Report of the Advisory Committee on Criminal Rules to the Committee on Rules of Practice and Procedure (May 2015).

39. U.S. CONST. amend. IV (protecting against unreasonable searches and seizures).

40. *Id.*

41. Smith v. Maryland, 442 U.S. 735, 740 (1979) (adopting the Katz v. United States, 389 U.S. 347 (1967) standard).

42. *Id.*; *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

43. *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) ("*Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search?").

44. *Katz*, 389 U.S. at 351 ("[w]hat a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.").

"knowingly exposes to the public."[45] This is the Third-Party Doctrine:[46] "where an individual makes information available to a third party, the government may obtain the information without a warrant, regardless of whether the act includes subjectively reasonable private behavior."[47] In essence, failing to keep an item or activity from being exposed to anyone but yourself risks losing the protection of the warrant requirement under the Fourth Amendment.[48] By exposing an activity to another party, you destroy the reasonable expectation of privacy and lose Fourth Amendment protections.

How the Third-Party Doctrine applies to modern technology is still up for debate.[49] *Smith* reasoned, "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone companies, since it is through telephone company switching equipment that their calls are completed."[50] Some lower courts equate this logic to IP addresses: "[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and from third parties, including [internet service providers]."[51] However, the Supreme Court has never definitively ruled on the issue.

ii. Objective Expectation of Privacy

Defendants must also have an objective expectation of privacy, the second part of the *Katz* test.[52] The expectation must be "one that society is prepared to recognize as 'reasonable.'"[53] Most importantly for the immediate topic, an objective expectation of privacy does not include any expectations of privacy in illegal activities. This

45. *Id.*

46. *See Smith*, 442 U.S. at 743-44 (no expectation of privacy in phone numbers dialed because they were turned over to the phone company).

47. Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 SANTA CLARA J. INT'L L. 104, 111 (2017).

48. *Id*.

49. United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People . . . can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.").

50. Smith v. Maryland, 442 U.S. 735, 742 (1979).

51. United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); *see also* United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008) (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register).

52. Katz v. United States, 389 U.S. 347, 361 (1967).

53. *Id*.

includes hijacking a neighbor's Internet access in order to share child pornography with a third party.[54]

3. Intrusion into a Constitutionally-Protected Area: Trespass

While modern courts focus on the reasonable expectation of privacy test from *Katz*, the original "trespass" test for the Fourth Amendment under *United States v. Jones* still stands.[55] *Jones* held that the Fourth Amendment protects against governmental, physical intrusion into a constitutionally protected area to obtain information.[56] Such actions constitute a "search" under the Fourth Amendment and are therefore subject to the warrant requirement.[57] For "trespass" analysis, expectation of privacy will not necessarily matter because the *Katz* reasonable expectation of privacy test adds to, but does not substitute for, the common-law trespassory test.[58] Essentially, *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern of government trespass upon protected areas.[59] Thus, there are circumstances where a governmental action fails to qualify as a "search" under the Fourth Amendment by the *Katz* test, but qualifies as a "search" under the *Jones*'s trespass analysis.[60]

4. The Exclusionary Rule – Suppression as a Remedy

The exclusionary rule was developed "[t]o deter Fourth Amendment violations."[61] When the Government seeks to admit evidence collected pursuant to an illegal search, the rule excludes (suppresses) that evidence, making it unavailable at trial.[62] While suppression is "a judicially created means of effectuating the rights secured

54. United States v. Stanley, 753 F.3d 114 (3d Cir. 2014).

55. *See* United States v. Jones, 132 S. Ct. 945 (2012); *see also* Florida v. Jardines, 569 U.S. 1 (2013) (extending Jones's trespass analysis to find law enforcement officers' use of drug-sniffing dog on front porch of home was a trespassory invasion of the curtilage which constituted a "search" for Fourth Amendment purposes).

56. *Jones*, 132 S. Ct. at 948–49; *see also* See United States v. Knotts, 460 U.S. 276, 285 (1983) (upholding against a Fourth Amendment challenge the use of a tracking device placed in a container of chloroform which was thereafter tracked because it was not a search or seizure).

57. *Jones*, 132 S. Ct. at 948–49.

58. *Jardines*, 569 U.S. at 5 ("By reason of our decision in Katz v. United States, property rights "are not the sole measure of Fourth Amendment violations,"—but though Katz may add to the baseline, it does not subtract anything from the Amendment's protections "when the Government does engage in [a] physical intrusion of a constitutionally protected area.") (citations omitted).

59. *Id.*

60. This distinction will come into play, *infra*, where courts struggle with whether the NIT counted as a "search" under *Katz* by comparing expectations of privacy in a defendant's IP address versus his computer. Further, it will show how the NIT failed to qualify as a tracking device under Federal Rule of Criminal Procedure 41(b)(4).

61. *See* United States v. Katzin, 769 F.3d 163, 169 (3d Cir. 2014).

62. *Id.*

by the Fourth Amendment,"[63] a Fourth Amendment violation does not result in automatic suppression.[64] Instead, "exclusion 'has always been [the court's] last resort, not [its] first impulse.'"[65] The court has consistently found the exclusionary rule is not an *individual* right. It applies only where it "'result[s] in appreciable deterrence.'"[66] Thus, where applying exclusionary rule would not deter the government from violating rights, the court will not apply the rule.[67]

Deterrent value alone is insufficient for application of the exclusionary rule.[68] The deterrent value must *also* outweigh the "substantial social costs" of exclusion.[69] Such costs "often include omitting 'reliable, trustworthy evidence' of a defendant's guilt, thereby 'suppress[ing] the truth and set[ting] [a] criminal loose in the community without punishment.'"[70] Because this result runs contrary to the truth-finding functions of the court, "exclusion is a bitter pill, swallowed only as a last resort."[71] Accordingly, violations warranting exclusion occur "where the deterrent value of suppression . . . overcome[s] the resulting social costs."[72]

5. The Good Faith Exception to the Exclusionary Rule

The Good Faith Exception to the exclusionary rule "was developed to effectuate [the balance between deterrent value and societal cost]."[73] The deterrent value of suppression tends to outweigh the costs "[w]here officers exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights."[74] However, when police act with an "objectively reasonable good-faith belief" in the legality of their conduct, or when their conduct "involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way."[75] Accordingly, discerning "whether the good faith exception applies requires courts to answer the 'objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light

63. Stone v. Powell, 428 U.S. 465, 482 (1976).

64. *See Katzin*, 769 F.3d at 170 (citing Herring v. United States, 555 U.S. 135, 140 (2009)).

65. Herring v. United States, 555 U.S. 135, 140 (2009) (quoting Hudson v. Michigan, 547 U.S. 586, 591 (2006)).

66. *Herring,* 555 U.S. at 141 (quoting United States v. Leon, 468 U.S. 897, 907 (1984)); *see also* United States v. Janis*,* 428 U.S. 433, 454 (1976)).

67. *Herring*, 555 U.S. at 141.

68. United States v. Katzin, 769 F.3d 163, 171 (3d Cir. 2014).

69. United States v. Leon, 468 U.S. 897, 907 (1984).

70. *Katzin*, 769 F.3d at 171

71. *Id*. (citations and internal quotation marks omitted).

72. *Id.*

73. *Id.* at 171.

74. *Id*. (quoting Herring v. United States, 555 U.S. 135, 144 (2009)).

75. *Id*.

of all of the circumstances.'"[76] In essence, egregious police violations of rights would tend to favor suppressing evidence to deter repetition of the police conduct. But when police act without gross misconduct and make a small mistake, the balance of deterrence compared to social cost weighs against the suppression of the wrongly obtained evidence.

6. Violations of Rule 41(b) and the Result

Rule 41(b) violations are categorized as either fundamental, when of constitutional magnitude, or technical, when not of constitutional magnitude.[77] Violations of Rule 41(b) that are of constitutional magnitude result in suppression of the evidence (unless some other exception applies).[78] In cases where a technical Rule 41(b) violation occurs, courts may suppress where a defendant suffers prejudice, "in the sense that the search would not have occurred. . .if the rule had been followed," or where law enforcement intentionally and deliberately disregarded the rule.[79]

C. Notable Cases and Judicial Analysis

In wrestling with Rule 41's magistrate jurisdiction requirement for warrants, technology, and the Fourth Amendment, the circuits have come to vastly different conclusions. The following cases highlight the divergence in reasoning, leading to findings in which NIT deployment is or is not a search depending on the jurisdiction. The cases also highlight the pre-amendment Rule 41(b) findings that allow or disallow magistrate issuance of NIT warrants dependent upon the jurisdiction.

1. Courts Finding Deployment of the NIT was not a "Search," but Result in Differing Rule 41(b) Analysis

In *United States v. Werdene*[80] and *United States v. Matish*,[81] both districts found that the use of the NIT did not constitute a Fourth Amendment search.[82] But, the courts diverged in their interpretation of Rule 41's restraint on magistrates' jurisdiction to

76. United States v. Katzin, 769 F.3d 163, 171 (3d Cir. 2014)

77. United States v. Negrete-Gonzales, 966 F.2d 1277, 1283 (9th Cir. 1995).

78. *See* United States v. Krueger, 809 F.3d 1109, 1113–14 (10th Cir. 2015) (ruling if a violation rises to the level of a Fourth Amendment violation, the violation can be considered constitutional in nature and suppression is warranted without further evidence of prejudice or reckless disregard. "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.").

79. United States v. Weiland, 420 F.3d 1062, 1071 (9th Cir. 2005).

80. 188 F. Supp. 3d 431 (E.D. Pa. 2016).

81. 193 F. Supp. 3d 585 (E.D. Va. 2016).

82. *Werdene*, 188 F. Supp. 3d at 443; *Matish*, 193 F. Supp. 3d at 613.

issue warrants.[83] While the courts reached opposite conclusions on Rule 41's conferral of jurisdiction, the outcome of the cases was essentially the same: denial of suppression of evidence.[84]

i. United States v. Gabriel Werdene- *Introduction*

After a magistrate in Virginia issued a warrant permitting deployment of the NIT, NIT data revealed the IP addresses of visitors to the Playpen website – including Gabriel Werdene.[85] Despite Werdene's use of TOR to conceal his IP and physical address, the NIT revealed that he lived in Pennsylvania. However, the NIT warrant came from an Eastern District of Virginia magistrate.[86] Werdene was indicted on September 17, 2015 on one count of possessing and attempting to possess child pornography pursuant to 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).[87] The indictment was based on evidence obtained during a June 17, 2015 search of Werdene's Bensalem, Pennsylvania home, which was conducted in accordance with a warrant issued by a magistrate judge in that judicial district (and based on probable cause stemming from use of the NIT).[88] Werdene moved to suppress the evidence seized from his home, arguing that under Rule 41 the magistrate judge lacked jurisdiction to authorize the NIT and the search of his IP address violated his Fourth Amendment rights.[89]

ii. Werdene– *Rule 41 and Jurisdiction*

The court found the Government's argument for a flexible application of Rule 41's jurisdictional conference unpersuasive, but found that no search under the Fourth Amendment had occurred.[90] Arguments that "Congress has not caught up with the changes in technology" and "Rule 41(b) is to be applied flexibly, not rigidly" were unsuccessful.[91] The simple fact was that in Werdene's case, the target of the NIT was located outside of the magistrate judge's district and beyond her jurisdiction under subsection (b)(1).[92] The property seized pursuant to the NIT warrant was not the server located in Newington, Virginia, but the IP address and related material "[f]rom

83. *Compare Werdene*, 188 F. Supp. 3d at 442–443*., with Matish*, 193 F. Supp. 3d at 612.

84. Throughout these cases, denial of suppression is the most prevalent result. *But see* United States v. Levin, 186 F. Supp. 3d 26, 36 (D. Mass. 2016).

85. *Werdene*, 188 F. Supp. 3d at 435.

86. *Id.*

87. *Id.* at 435.

88. *Id.*

89. *Id.* at 436.

90. *Id* at 442–43.

91. United States v. Werdene, 188 F. Supp. 3d 431, 442–43 (E.D. Pa. 2016).

92. *Id.*; *see supra* Part I.B.1.

any 'activating' computer" that accessed Playpen.[93] The material was located outside of Virginia, so the magistrate did not have authority to issue the warrant under Rule 41(b)(1).[94] Likewise, Subsections (b)(2) and (b)(4) (the tracking provision), the only other provisions potentially applicable, were premised on the person or property being located within the issuing court's district.[95] It was uncontested that the computer information that the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia.[96] Therefore, the magistrate judge was accordingly without authority to issue the NIT warrant.[97]

However, the court concluded that because Werdene did not have a reasonable expectation of privacy in his IP address, the NIT used by government was not a "search" under the Fourth Amendment.[98] Therefore, the magistrate's violation in issuing extra-territorial warrants was not a constitutional concern.[99] Nor was Werdene's subjective expectation of privacy reasonable.[100] His expectation was not "[a subjective expectation] that *society* is prepared to recognize as 'reasonable.'"[101] Werdene failed both parts of the *Katz* reasonable expectation of privacy analysis.[102]

The court concluded that assuming Werdene had a reasonable expectation of privacy in the information obtained by the NIT, suppression was not the appropriate remedy.[103] Because exclusion is not a personal right and not guaranteed by the Constitution,[104] application of the exclusionary rule is "limited to those 'unusual cases' in which it may achieve its objective: to appreciably deter governmental violations of the Fourth Amendment."[105] That deterrent value must outweigh social costs of excluding the evidence.[106]

93. *Werdene*, 188 F. Supp. 3d at 442–43.

94. *Id.*; *compare id.,* with United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016) (holding the magistrate had authority to issue the warrant under 41(b)(4)).

95. *Werdene*, 188 F. Supp. 3d at 442.

96. *Id.*

97. *Id.*

98. *Id.* at 443 ("Specifically, he must articulate how the Government's failure to comply with Rule 41(b) caused a search or seizure prohibited by the Fourth Amendment. He cannot do so.").

99. *Id.*

100. *Id.* at 445.

101. United States v. Werdene, 188 F. Supp. 3d 431, 445 (E.D. Pa. 2016)

102. *Id.* at 446

103. *Id.* at 448.

104. *Id*. citing Davis v. United States, 564 U.S. 229, 236, 285 (2011) (exclusion was not "designed to 'redress the injury' occasioned by an unconstitutional search.") (citation omitted); *see* Hudson v. Michigan, 547 U.S. 586, 591–92 (2006) (whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's Fourth Amendment rights were violated).

105. *Werdene*, 188 F. Supp. 3d, at 448 (quoting United States v. Katzin, 769 F.3d 163, 170 (3d Cir. 2014)); *see generally*, *supra,* Part II.B.

106. *Werdene*, 188 F. Supp. 3d at 448.

Following that logic, even if deployment of the NIT was a search and violated Rule 41, the Good Faith Exception to the exclusionary rule applied. Because the FBI acted "upon an objectively reasonable good faith belief in the legality of their conduct," the court essentially would not punish the FBI for relying in good faith on the warrant.[107]

iii. United States v. Matish - *Introduction*

Like in *Werdene,* prosecution of Edward Matish stemmed from the Government's investigation into the child pornography website, Playpen.[108] Matish accessed Playpen via TOR in an attempt to keep his IP address anonymous.[109] Following the deployment of the NIT, the FBI determined Matish's IP address and sent a subpoena to his ISP, which identified the computers that possessed that IP address on a particular date and time.[110] Based on this information, the local magistrate authorized a residential search warrant for Matish's home, which the FBI executed on July 29, 2015.[111] Pursuant to this second warrant, the FBI seized several computers, hard drives, cell phones, tablets, and video game systems.[112]

On February 8, 2016, Matish was named in a four (4) count criminal indictment charging him with access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5) and (b)(2).[113] These charges stemmed from the information collected by the NIT, which had provided probable cause for the warrant to search his home.[114] Matish then filed motions to suppress.[115]

iv. Matish– *Rule 41 and Jurisdiction*

The court in *Matish* ultimately concluded use of the NIT was not a search. Thus, a NIT deployment did not require a warrant.[116] However, the court found Rule 41(b)(4)

107. *Id.* at 451–52 (observing: (1) the magistrate believed that she had jurisdiction to issue warrant but mistakenly issued it outside her jurisdiction; (2) agents did not misrepresent how search would be conducted or where it would be conducted; (3) agents otherwise acted upon objectively reasonable good faith belief in legality of their conduct; (4) suppression would not have any appreciable effect on law enforcement; and (5) government's evidence against defendant was substantial but the government would not have any case without it.).

108. United States v. Matish, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

109. *Id.* at 593–94.

110. *Id.* at 595–96.

111. *Id.* at 596.

112. *Id*.

113. *Id.* at 592.

114. United States v. Matish, 193 F. Supp. 3d 585, 596 (E.D. Va. 2016).

115. *Id.*

116. *Id.* at 618.

authorized the issuance of the NIT warrant.[117] Rule 41(b)(4) *endowed* a magistrate with authority to issue a warrant authorizing the use of a tracking device.[118] The tracking device must be installed within the magistrate judge's district, but 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."[119]

The court analogized that provision of Rule 41(b)(4) and adapted it to the virtual world. Whenever a user entered Playpen, he made "a virtual trip" via the Internet to Virginia.[120] Because the NIT enabled the Government to determine Playpen users' locations, it resembled a tracking device.[121] The court's technical analysis asserted that installation did not occur on the government-controlled server but on each individual computer that logged into Playpen (in the Eastern District of Virginia).[122] When that user logged out of Playpen, the NIT determined the location, just as traditional tracking devices inform law enforcement of a target's location.[123] Thus, Rule 41(b)(4) applied because this situation was analogous to a tracking device installed in Virginia which then left the state.[124]

Matish also held that even if issuing the warrant extended beyond the magistrate's control, no Fourth Amendment violation occurred.[125] The Government did not need a warrant to capture the defendant's IP address because collecting IP addresses was not a search.[126] The defendant transferred his IP addresses to a third party – the TOR node or ISP – so he had no reasonable expectation of privacy in it.[127] The warrant, even if invalid or void, was unnecessary.[128] Specifically, the court found that IP addresses are information revealed to a third party: "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[129] Generally, a user has no reasonable expectation of privacy in an IP address when using the Internet.[130] This stems from the fact that

117. *Id.* at 612. *Compare id.*, *with* United States v. Werdene, 188 F. Supp. 3d 431, 442 (E.D. Pa. 2016) (holding that none of the applicable Rule 41(b) provisions conferred jurisdiction to a magistrate for an NIT warrant).

118. *Matish*, 193 F. Supp. 3d at 612.

119. *Id*.

120. *Id.* at 612–13.

121. *Id.* at 613.

122. *Id.*

123. *Id.*

124. United States v. Matish, 193 F. Supp. 3d 585, 613 (E.D. Va. 2016).

125. *Id.* at 613–14.

126. *Id.*

127. *Id.* at 615.

128. *Id.* ("Generally, one has no reasonable expectation of privacy in an IP address when using the Internet."); *see*, *e.g.*, United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2007).

129. *Matish*, 193 F. Supp. 3d at 614 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

130. *Id.* at 615 (quoting *Forrester*, 512 F.3d at 509–11).

Internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[131] In essence, the *Matish* court recognized IP addresses are turned over to third parties and so there is no reasonable expectation of privacy in them.[132] Because there was no expectation of privacy, the Fourth Amendment did not apply and the FBI needed no warrant.[133] Effectively, the warrant obtained was a bonus.

The Court noted that TOR users might have a *subjective* expectation of privacy arising from their use of the network, but they must disclose information, including their IP addresses, to unknown individuals running TOR nodes to direct their communications toward their destinations.[134] Further, the TOR Project warns users "that the TOR network has vulnerabilities and that users might not remain anonymous."[135] Thus, there was no objectively reasonable expectation of privacy.[136] When a user connects to the TOR network, he or she must disclose his or her actual IP address to the first TOR node with which he or she connects.[137] Coupled with the TOR Project's own warning that the first server can see "[t]his IP address is using TOR" destroys any expectation of privacy in a TOR user's IP address.[138]

The court also ruled that TOR users do not have a reasonable expectation of privacy in their computers and thus got around the maxim that "the appropriate [Fourth Amendment] inquiry [is] whether the individual had a reasonable expectation of privacy in the area searched, not merely in the items found."[139] The NIT collected very limited information.[140] Moreover, the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy.[141]

131. *Forrester,* 512 F.3d at 510.

132. *Matish*, 193 F. Supp. 3d at 614.

133. *Id.*

134. *Id.* (emphasis added).

135. *Id.* at 616–617.

136. *Id*.

137. United States v. Matish, 193 F. Supp. 3d 585, 617 (E.D. Va. 2016).

138. *Id.*

139. *Id.* (quoting United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir.1986)).

140. *Id.* at 618 (analogizing the NIT to the pen register in *Smith* that only captured the numbers dialed, "The NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer."). *Cf.* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

141. *Matish*, 193 F. Supp. 3d at 619 ("[h]acking is much more prevalent now than it was even nine years ago, and the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy. . . Now, it seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked."). Given the prevalence of hacking, the court analogized breach of Apple's private data to TOR users hoping to keep their network information private. ("TOR users likewise cannot reasonably expect to be safe from hackers. Even if TOR users hope that the TOR network

Lastly, *Matish* reasoned that even if a warrant was needed, the Good Faith Exception applied and suppression should be denied.[142] The agents' reliance on the NIT warrant was objectively reasonable, and it appeared to the Court that the agents acted in good faith.[143] The agents did not lie to the magistrate, the warrant application detailed ample probable cause to support the issuance of the warrant, and the affidavit adequately described the items to be seized and the places to be searched.[144]

2. Where the Court Found Deployment of the NIT was a "Search"

Circuit courts disagreed as to whether or not the un-amended Rule 41(b) granted a magistrate jurisdiction for NIT warrants.[145] But more importantly, they still disagree whether deployment of the NIT constitutes a search under the Fourth Amendment.[146] This split stems from the courts' focus either on the mere collection of the IP addresses versus the government intrusion onto defendants' computers.[147] In general, the courts that focus on the IP address note that there is no expectation of privacy in IP addresses because of the Third-Party Doctrine and therefore no search has occurred.[148] Conversely, courts that focus on the NIT's intrusion onto a defendant's computer as a constitutionally-protected area usually characterize NIT deployment as a search.[149] Regardless of whether the court concludes there was a search or not, suppression of the evidence is rarely granted as a remedy.[150]

will keep certain information private—just as terrorists seem to expect Apple to keep their data private—it is unreasonable not to expect that someone will be able to gain access.").

142. *Id.*

143. *Id.*

144. *Id.*

145. *See supra* note 31 and accompanying text.

146. *See generally Matish*, 193 F. Supp. 3d at 616–617; *see infra* notes 150–159 and accompanying text.

147. *Compare* United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016) *with Matish,* 193 F. Supp. 3d at 616–617.

148. *See* United States v. Werdene, 188 F. Supp. 3d 431, 443 (E.D. Pa. 2016); *see also Matish*, 193 F. Supp. 3d at 615; United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016); United States v. Lough, 221 F. Supp. 3d 770, 775 (N.D. W. Va. 2016).

149. *See* United States v. Darby, 190 F. Supp. 3d 520, 528–29 (E.D. Va. 2016); *Adams*, 2016 WL 4212079, at *4 ("However, Defendant's IP address was discovered only after property residing within Defendant's home—his computer—was searched by the NIT. The courts which have thus far grappled with the extent to which a person has a reasonable expectation of privacy in an IP address have analyzed the issue in the context of a subpoena to an ISP to identify the person assigned the IP address."); United States v. Ammons, 207 F. Supp. 3d 732, 738–39 (W.D. Ky. 2016); United States v. Broy, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016).

150. *See supra* note 33 and accompanying text; United States v. Croghan, 209 F. Supp. 3d 1080, 1085-86 (S.D. Iowa Sept. 19, 2016), *rev'd and rem'd by* United States v. Horton 863 F.3d 1041 (July 24, 2017) and United States v. Levin, 186 F. Supp. 3d 26, 36 (D. Mass. 2016) are currently some of the few cases that granted suppression. The district court in *Croghan* was overturned and it is probable that the Levin decision was an error because they relied on authority (United States v. Scott, 260 F.3d 512 (6th Cir. 2001)) that the Sixth Circuit itself

i. United States v. Adams

Like the previous cases, the United States charged Ryan Anthony Adams with receipt and possession of child pornography stemming from the Playpen investigation.[151] Adams used TOR to access the website and conceal his IP address. The FBI used the NIT to collect Adams's IP address on February 20, 2015.

While the court noted that Adams did not have a reasonable expectation of privacy in the IP address used to access Playpen,[152] the court noted that the NIT obtained Adam's IP address by searching his computer.[153] Once a user's computer downloads the content from Playpen, the NIT causes the user's computer to transmit information to a computer controlled by the Government.[154] Essentially, the NIT travels to the user's computer and identifies the IP address and other information before transmitting it back to a government-controlled computer.[155] Thus, the *Adams* court noted that the question of a search under the Fourth Amendment would turn on whether the IP address should be the focus of the analysis or if Adam's expectation of privacy in his computer is the proper subject of analysis.[156]

Because Adam's IP address was discovered only after property residing within his home (the computer) was searched by the NIT, the court concluded the expectation of privacy *in the device* is the proper focus of the analysis, and not one's expectation of privacy in the IP address residing in that device.[157] The court reasoned that other courts grappling with the reasonable expectation of privacy in an IP address have analyzed the issue in the distinguishable context of a subpoena to an ISP.[158] Instead, *Adams* disagrees with *Werdene* improperly mixing the lack of expectation of privacy associated with an IP address with the expectation of privacy one has in the computer itself.[159] Therefore, because the NIT searched Adam's computer (which he did have a reasonable expectation of privacy) to get the IP address (for which there was no reasonable expectation of privacy), deployment of the NIT constituted a search under the Fourth Amendment.[160]

admits was "effectively reversed" in United States v. Master, 614 F.3d 236 (6th Cir. 2010). The Levin decision is currently on appeal).

151. *Adams*, 2016 WL 4212079, at *1.

152. *Id*. at *4.

153. *Id.*

154. *Id.*

155. *Id.*

156. *Id.*

157. United States v. States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016) (emphasis added).

158. *Id.*

159. *Id.*

160. *Id.*

II. ANALYSIS

Given the current precedent, a magistrate originally did not have the authority to issue an NIT warrant outside of her jurisdiction.[161] Court opinions holding otherwise were in error.[162] However, after the amendment of Rule 41 and addition of subsection (b)(6), now magistrates certainly do have that jurisdiction.[163] The only question remaining is if deployment of the NIT constitutes a search under the Fourth Amendment requiring the issuance of such a warrant. The use of the NIT constitutes a search under the Fourth Amendment, even if it only collects information like IP addresses routinely given to third parties.[164] The following section will attempt to justify these positions and will conclude the amendment of Rule 41 may influence the "search or no search" analysis going forward.

A. NIT Warrant Jurisdiction and Classification as a "Search"

Despite contrary holdings, under the pre-amended Rule 41(b)(6), a magistrate did not have jurisdiction to issue a warrant for electronic NIT search extending outside his jurisdiction.[165] Findings of pre-amendment jurisdiction were justified by subsections (b)(1) and (b)(4).[166] The following addresses why these provisions of the pre-amended Rule 41(b) failed to grant jurisdiction to a magistrate for an NIT search.

Subsection (b)(1) is straightforward: a magistrate judge may authorize the search or seizure of property within the district in which the judge sits.[167] Most courts justifying magistrate jurisdiction of the NIT warrant via pre-amendment Rule 41(b) disregard subsection (b)(1).[168] Typically, courts note that the NIT warrant authorizes

161. *See supra* Part I.B.1.

162. If the courts holding deployment of the NIT fell within the previous rule were correct, it would at the least beg the question of why an amendment to Rule 41(b) was necessary.

163. *See* FED. R. CRIM. P. 41(b)(6).

164. *See infra* notes 190–209 and accompanying text.

165. *But see* United States v. Jean, 207 F. Supp. 3d 920 (W.D. Ark. 2016); United States v. Eure, No 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016); United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016); United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016). The stretching of Rule 41's conferral of jurisdiction can likely be rationalized by the court's unwillingness to suppress condemning evidence for such an emotionally charged crime like child pornography. Additionally, almost all courts that found the warrant outside of the magistrate's authority nonetheless refused suppression because of the Good Faith Exception.

166. *See Matish*, 193 F. Supp. 3d at 612.

167. *See* United States v. Chipps, 410 F.3d 438, 446 (8th Cir. 2005); *see also* United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437, at *2 (E.D. Tenn. Apr. 2, 2010) ("Rule 41(b). . . limits a Magistrate Judge's authority to issue warrants only for property within the district."); United States v. Hernandez, No. 3:08-CR-142, 2008 WL 4748576, at *16 (D. Minn. Oct. 28, 2008) ("[T]he jurisdiction of a United States Magistrate Judge which, as a general proposition, is limited to the District in which he or she sits.").

168. *See generally* United States v. Levin, 186 F. Supp. 3d 26, 35 (D. Mass. 2016); United States v. Michaud, No. 3:15–CR–05351–RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016).

the NIT to "obtain information . . . from the activating computers."[169] Nearly all disputes arising from these cases have had activating computers located outside the magistrate's jurisdiction, the Eastern District of Virginia. [170] The courts generally held the defendant's computer, not the server located in Virginia, was the location searched.[171] Therefore, Rule 41(b)(1) did not authorize those searches because the place to be searched and information to be seized were located outside of the issuing court's jurisdiction.[172] This reasoning is sound. Even if the government attempted to characterize the search as occurring in Virginia, what information could they obtain from their own server? The NIT may have waited for connections on the server in Virginia before downloading itself to an outside system, but that installation occurred outside the issuing jurisdiction. The NIT searches were after information only the NIT deployment could produce, namely IP addresses.[173] That information came from outside the jurisdiction, not from the mere deployment of the NIT on the Virginia server.[174]

The next commonly attempted route to secure jurisdiction for the NIT warrant is Rule (41)(b)(4).[175] That subsection provides:

> "[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[.]"[176]

169. *See* United States v. Workman, 205 F. Supp. 3d 1256, 126 (D. Colo. 2016), *rev'd by* United States v. Workman 863 F.3d 1313 (2017).

170. *See Levin*, 186 F. Supp. 3d at 35 (finding that the NIT Warrant was not authorized by Rule 41(b)(1) where the defendant's computer was located in Massachusetts); *Michaud*, 2016 WL 337263, at *6 (holding that the NIT Warrant was not authorized by 41(b)(1) "because the object of the search and seizure was [the defendant's] computer, not located in the Eastern District of Virginia.").

171. *See Levin*, 186 F. Supp. 3d at 35.

172. For cases arising from the NIT search that unmasked residents of Virginia, it is arguable that the jurisdiction of the warrant is satisfied by Rule 41(b)(1). However, such a warrant may face particularity challenges, as almost all the challenges to the NIT warrant have. After all, the FBI did not know the location to be searched, since the location was concealed. How then could they state with particularity the place to be searched?

173. *See supra* note 7 and accompanying text.

174. *See* United States v. Werdene, 188 F. Supp. 3d 431, 438 (E.D. Pa. 2016) ("[T]he NIT may cause an activating computer—wherever located—to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer.").

175. *See* United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016); *Werdene*, 188 F. Supp. 3d at 442.

176. FED. R. CRIM. P. 41(b)(4).

Further, the federal rules define "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[177]

Circuits have split over analogizing the NIT to a tracking device.[178] Courts disregarding a (b)(4) tracking analogy, note that the NIT was never installed in the issuing jurisdiction, as required by the statute.[179] Proponent courts argue the NIT *was* installed in Virginia.[180] However, both courts overlook a more fundamental question: whether the NIT actually "tracked" at all.

Subsection (b)(4) should have been confined to physical tracking: its original purpose. To bootstrap Rule 41(b)(4) into NIT searches stretches the realm of what counts as "tracking" beyond its design. Tracking devices are traditionally thought of as physical beacons placed on physical objects that monitor location over time.[181] The NIT, however, clearly did not "track" the "movement of a person or object."[182] In fact, the NIT did not "track" the "movement" of anything, but rather it installed computer code onto defendants' computers, which then caused the computers to relay the IP addresses to the government-controlled computers in Virginia.[183] The FBI subsequently subpoenaed the physical location of the IP address from the ISPs.[184] Thus, because the NIT is not an electronic device that permits the "tracking" of the movement of a person or object,[185] the language of Rule 41 and the statutory definition of "tracking device" do not support qualifying use of the NIT as a tracking device.[186]

Moreover, courts characterizing the NIT installation as occurring in Virginia were misguided. The NIT was uploaded to the Virginia server, but it did nothing until downloaded to the suspects' computer, decidedly outside Virginia in nearly all

177. FED. R. CRIM. P. 41(a)(2)(E).

178. *See supra* Part I.C.1; *Compare Werdene*, 188 F. Supp. 3d 431 at 442 *with Matish*, 193 F. Supp. 3d at 593 (where the court held the magistrate had authority to issue the warrant under 41(b)(4)). For cases holding (b)(4) failed to confer jurisdiction see *supra* note 31 and accompanying text.

179. *See generally Werdene*, 188 F. Supp. 3d 431; FED. R. CRIM. P. 41(b)(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 . . . *outside the district*").

180. *Matish*, 193 F. Supp. 3d at 593.

181. *See generally* United States v. Jones, 132 S. Ct. 945 (2012).

182. *See supra* note 77 and accompanying text.

183. United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016).

184. *Id.*

185. *See* FED. R. CRIM. P. 41(a)(2)(E).

186. *Id; see* FED. R. CRIM. P. 41(b)(4). For the multitude of cases arising out of the use of the NIT, the FBI's *modus operandi* has generally been the same: deploy the NIT and retrieve the suspect's IP address. Subpoena the ISP for the suspect's physical location using the IP address. Apply for a search warrant of those premises based on probable cause obtained from the NIT.

cases.[187] Installment of the NIT on the government-controlled server is analogous to the government possessing a physical tracking device. When the device is in government possession and under its control, it cannot be said to have been installed and tracking the defendant. For purposes of analogy, this would be akin to the government in *Jones* claiming that since it had the tracking device in its possession in the warranted district, it was installed for the purposes of (b)(4).[188] Simply put, you cannot have a tracking device installed in a district without it actually being deployed.

Defendants electronically contacted the server while maintaining their physical location outside the jurisdiction.[189] When the NIT was deployed by the FBI it was subsequently installed on the computers located outside of Virginia.[190] That is, when the NIT actually was deployed then it began "tracking," if it can be argued it "tracked" at all. In sum, a piece of code sitting on a government server in a particular district cannot be said to have been deployed on a defendant residing outside that district. The NIT remained un-deployed in Virginia until the defendants' computer reached out to it. Only then was it installed, but outside the jurisdiction.

1. Deployment of the NIT is a Search—Collection of IP Addresses is Not.

Many circuits held the NIT collection of IP addresses is not a search under the Fourth Amendment.[191] Such analysis disregards the true hinge point*: while IP addresses have no expectation of privacy, the computers that are accessed do*. The analysis turns on whether the courts focus on the location searched or the information collected.[192] Because the NIT intrudes into an area that has a reasonable expectation

187. *See* United States v. Michaud, No 3:15–cr–05351–RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016); *Adams*, 2016 WL 4212079, at *6.

188. *See* United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016) ("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).").

189. United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016). *But see* United States v. Sullivan, 229 F. Supp. 3d 647,654 (N.D. Ohio 2017) (adopting other circuits' reasoning where the defendant digitally visited, or "touched down" in Virginia and thus the search took place there); United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016).

190. *See Michaud*, 2016 WL 337263, at *6; *Adams*, 2016 WL 4212079, at *6.

191. *See supra* Part I.C.1.

192. After all, as one court has analogized, if the government were to break into your locked garage to find the car you had stolen, it would surely be a search. The fact that you had no expectation of privacy in a stolen car would not diminish your expectation of privacy in your home. Likewise, intruding into and pulling information from a computer (which has an expectation of privacy) that is in a defendant's home would be just as much a search. *See Adams*, 2016 WL 4212079 at *4 ("For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the

of privacy, courts that hold collecting IP addresses via the NIT do not constitute a search are in error.

i. IP Addresses Have No Expectation of Privacy

IP addresses are information voluntarily transmitted to third parties like pen registers from *Smith v. Maryland*.[193] Thus, defendants' have no reasonable expectation of privacy in them. Without an expectation of privacy, there is no Fourth Amendment implication and therefore no "search."

In the present cases:

(1) TOR warned *Werdene* and *Matish* their connection was not completely secure.[194] This would remove a subjective manifestation of privacy. If they were warned they were not secure, they couldn't be said to have subjectively believed they were private. Analogously, imagine that a neighbor warned you of a hole in your fence that passed along the sidewalk so that anyone might look through and see into your yard. In such a case, the subjective manifestation of privacy in your yard given by the fence would be negated.

(2) *Werdene* and *Matish* knew the TOR connection forwarded their IP address to the first node in the TOR chain.[195] This is a fatal flaw in the TOR coffin of expectation of privacy. The defendants turned over their IP address to a telecommunication company like in *Smith* (which is enough to negate Fourth Amendment concerns), but also forwarded their IP addresses to a third party.[196] This is akin to telling a stranger what your IP address is. Because a person has no legitimate expectation of privacy in information, he voluntarily turns over to third parties, *Matish* and *Werdene* cannot assert an expectation of privacy in their IP address when transferred via TOR.[197]

(3) Lastly, society is not likely to find their subjective expectation objectively reasonable, especially for child pornography distribution purposes. This means there is no objective expectation of privacy.

ii. Computers Have an Expectation of Privacy and Should be the Benchmark

Despite a lack of an expectation of privacy in IP addresses, deploying the NIT on a defendant's computer is a search because there is a reasonable expectation of privacy in personal computers. Viewing NIT collection of data from a computer as a

"open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device.").

193. *See supra* Part I.C.1 (outlining cases finding that deployment of the NIT did not constitute a search).

194. *See supra* Part I.C.1 (outlining cases finding that deployment of the NIT did not constitute a search).

195. *Id.*

196. *Id.*

197. *See supra* Part I.B.2.

non-search overlooks the fact that courts have consistently treated private computers on par with closed containers[198] and overlooks the location of the search for the subject of the search. Because individuals have a reasonable expectation of privacy in the contents of closed containers,[199] defendants also generally retain a reasonable expectation of privacy in data held within electronic storage devices.[200] Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable expectation of privacy in the information. A defendant's IP address is, by definition, information stored on their computer.[201] Therefore, while defendants do not have an expectation of privacy in their IP address, the government infringed upon the expectation of privacy in their computers by deploying the NIT. Because the NIT searches a defendant's computer to discover the IP address, the expectation of privacy in the computer is the correct focus of the analysis.

Reliance on the Third-Party Doctrine to hold collection of IP addresses via the NIT as not a search mischaracterizes the nature of the doctrine. In every instance where the court has upheld third party arguments, the information has been transmitted by a third party to the government.[202] What has not occurred is the government merely noting information collected is *likely* to be transmitted to a third party and then directly collecting it themselves.[203] By skipping the third party "middle man," the FBI in fact receives its information from the NIT via its own efforts, not a third-party ISP. When the FBI claims to use the Third-Party Doctrine with the NIT, there is no third party involved, merely the defendant and the FBI. That the IP address might at some time be transmitted to an ISP does not diminish this fact.

198. *See* H. MARSHALL JARRETT & MICHAEL W. BAILIE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 3 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf; *see also* United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."); United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001) (assuming that computer disks are containers and subject to standards governing closed container searches); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (finding that Fourth Amendment protection of closed computer files and hard drives is similar to protection afforded closed containers and closed personal effects); United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("A personal computer is often a repository for private information the computer's owner does not intend to share with others. *For most people, their computers are their most private spaces.*" (internal quotation omitted) (emphasis added)).

199. *See* United States v. Ross, 456 U.S. 798, 822–23 (1982).

200. *See supra* note 152 and accompanying text.

201. At least, the NIT cannot access and transmit the IP address without being downloaded to the computer.

202. Brief of Professor David Gray as Amicus Curiae, Maryland v. Kerron Andrews, 227 Md. App. 350 (2016) (No. 1496); *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976); Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966).

203. *See* Smith v. Maryland, 442 U.S. 735, 737 (where the telephone company voluntarily cooperated with law enforcement in installing pen registers and turning that information over to police).

Besides infringing on an expectation of privacy, deploying the NIT can be considered a search under trespass analysis.[204] For trespass purposes, when "the Government obtains information by physically intruding" on persons, houses, papers, or effects, "a 'search' within the original meaning of the Fourth Amendment" has "undoubtedly occurred."[205] A computer has its own expectation of privacy and is almost always located inside a defendant's home.[206] Moreover, a computer is definitely a "paper" or "effect" for the purpose of the Fourth Amendment.[207] Thus, when the NIT is deployed onto a computer, it is not only intruding into the home, but also into the papers or effects contained in the computer. The only barrier for NIT under trespass analysis is the "physical" intrusion. It is true that the NIT code does not literally walk into the home's curtilage like officers in *Florida v. Jardines*,[208] nor is it installed on a car like in *Jones*.[209] However, it would be incongruous of courts to both hold that the NIT is analogous to a tracking device under 41(b)(4) and then deny it is a search like the tracking device utilized in *Jones*. More, on a fundamental level, deploying the NIT changes the code on the defendant's computer, an act that necessarily transforms some physical aspect of its hard drive or memory.[210] Thus, the deployment of the NIT can be considered a "physical" intrusion under trespass analysis.

2. Suppression is Unwarranted Regardless

Even if the collection of IP addresses was considered a search and the warrants issued were illegitimate, the Good Faith Exception would apply. FBI agents acted reasonably on their issued NIT warrant and relied on it for legitimacy of the search. Thus, suppressing the evidence would do nothing to deter them from the conduct of

204. *See* Florida v. Jardines, 133 S. Ct. 1409 (2013); *supra* PartI-B-2.

205. *Jardines*, 133 S. Ct. at 1414.

206. *See infra* note 206 and accompanying text (outlining cases noting that computes are "effects" for Fourth Amendment analysis).

207. United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (explaining that "private information individuals store on digital devices" are "personal 'papers' in the words of the Constitution."); United States v. Christie, 717 F.3d 1156, 1164 (10th Cir. 2013) (noting personal computers "contain (or at least permit access to) our diaries, calendars, files, and correspondence – the very essence of the 'papers and effects' the Fourth Amendment was designed to protect."); United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009) ("[c]omputers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives.").

208. 133 S. Ct. 1409 (2013).

209. 132 S. Ct. 945 (2012).

210. Chris Woodford, *Hard Drives*, EXPLAIN THAT STUFF (Apr. 3, 2017) http://www.explainthatstuff .com/harddrive.html (most permanent information on computers is stored in binary bits in the hard drive. Injecting the NIT into a suspect's computer necessarily changes at least part of the suspect's computer memory or code).

the search. Deterrence of law enforcement misconduct is the foundational justification behind the suppression remedy.[211] Without deterrence, there will be no suppression.[212] After all, what more could the FBI have done? Before the amendment of Rule 41, the FBI had no other way to obtain a warrant for outside of Virginia because they did not know the sources of Playpen's incoming connections.[213] Incoming connections could be from anywhere in the world, not just the jurisdiction of Virginia where the server was located. Given that, punishing the FBI by suppressing the evidence would be a fruitless endeavor, merely chastising them for something they could not change.

B. Effects of the Amendment of Rule 41(b)

With the Rule 41 amendment, including any jurisdiction where the originating jurisdiction has been concealed through electronic means (i.e. via TOR), the FBI need not worry about having its warrants struck for jurisdiction. Essentially, the amendment resolved the *Werdene/Matish* debate about Rule 41 electronic jurisdiction with a stroke of the pen.[214] But could the adaptation of Rule 41 have farther-reaching consequences? The amendment allowed for the issuance of warrants but did not resolve the question whether NIT deployment is a search.[215] However, why would the Supreme Court promulgate rules explicitly granting the power to issue such warrants across jurisdictions if the underlying action is not a search? There are a few reasons. First, the amended rule merely fixed a circuit split.[216] By amending the Rule, courts will not stress over whether a magistrate has jurisdiction and suppression will not be an issue.[217] Second, the Court amended the Rule to allow such warrants so that computers themselves can be searched with probable cause when they are technically outside the magistrate's jurisdiction.[218] With the new Rule 41 (b)(6), a magistrate could find probable cause and essentially allow the FBI to hack a computer outside the jurisdiction if it is concealed via electronic means.[219]

211. *See supra* note 65 and accompanying text.

212. *See supra* note 65 and accompanying text.

213. *See generally* NIT Warrant Affidavit, *supra* note 1.

214. *See supra* note 37 and accompanying text (Advisory Committee noting the 41(b) amendment resolved increasing territorial restrictions caused by electronic concealment).

215. *See supra* note 37 and accompanying text (Advisory Committee noting the 41(b) amendment resolved increasing territorial restrictions caused by electronic concealment).

216. Such circuit splits were becoming more pronounced before the Rule's amendment. *See supra* note 31, 37 and accompanying text.

217. *See* FED. R. CRIM. P. 41(b)(6). Much of the NIT litigation stems from the issuing magistrate's warrant jurisdiction. If the magistrate clearly has jurisdiction via Rule 41(b)(6), the Fourth Amendment will be satisfied for the NIT "searches." *See* United States v. Levin, 874 F.3d 316, 321 n.3 (2017).

218. *See* FED. R. CRIM. P. 41(b)(6) (allowing the issuance of a warrant where the district where the media or information is located has been concealed through technological means).

219. *Id.*

This reasoning represents a massive shift, but not an undue one in the case of child pornography. Or third, the Court could be considering a revision to the idea of a "search" in the electronic age. In her concurrence in *Jones*, Justice Sotomayor noted that perhaps the Court should revisit *Smith* in light of the electronic age.[220] The change in Rule 41 could be the beginning of that revisitation. *After all, why would the Court allow issuing a warrant for an action that was not a search?* If deploying the NIT onto computers, which have a legitimate expectation of privacy, is not a search under the Fourth Amendment, why amend the rule to allow a warrant issuance? Indeed, what will the present impact be if the FBI remotely searches computers concealed by TOR via the NIT without a warrant? Arguably, they were originally a search, but the lack of a warrant would persuade courts originally focusing on the mere collection of IP addresses to understand that the true focus should be the search of the computer. The situation is a conundrum – the defense can ask the FBI why it did not get a warrant for a remote computer search, yet point out specifically there is a rule that allows the issuance of a warrant for such collection.

The amendment of Rule 41 also may affect the reliance of the Good Faith Exception. With the change, the Good Faith Exception is a stronger defense than ever. Warrants issued under Rule 41(b)(6) will ease the authorization of cross-jurisdictional electronic data collection where the suspect's location is concealed via electronic means.[221] In effect, the FBI would not need the Good Faith Exception. Instead, the warrant will stand on its own feet.

CONCLUSION

With the amendment of Rule 41(b)(6), the question of magistrate power to issue NIT warrants outside his jurisdiction has been resolved. What remains a question is whether courts will come to a consensus on the question of deploying the NIT. Does its deployment constitute a search? The nation adopted the Fourth Amendment out of fear of a general warrant that would allow law enforcement to search anyone, anywhere, anytime – and eliminate privacy in our persons, papers, and effects. If the NIT is found not to be a search, it may be the beginning of a new electronic age of general warrants, one in which the FBI can implant code on a person's computer and pull information from it without restriction by the warrant requirement and probable cause. The shift may mean warrants collecting IP addresses today could morph to collect personal documents, pictures, or more tomorrow.

220. *See supra* note 48 and accompanying text.

221. *See supra* note 207 and accompanying text.