DICING THE ONION: AN ANALYSIS OF TRANS-JURISDICTIONAL WARRANTS REGARDING ANONYMOUS CYBER CRIMINALS

Bryan Mercke[*]

I. INTRODUCTION

Alex Levin, a Maryland resident, was charged with possession of child pornography after an FBI search of his computer found incriminating evidence.[1] In May of 2016, Levin successfully suppressed the evidence found on his computer by urging that the Virginia magistrate judge's warrant lacked jurisdiction and violated the Federal Rules of Criminal Procedure 41(b) (Rule 41).[2] In a prescient move by the Supreme Court, Rule 41 was amended in December 2016 to allow magistrate judges to issue warrants across jurisdictions when anonymizing tools are used to hide a cyber criminal's identity.[3]

The issuance of trans-jurisdictional warrants regarding illicit online activity has sparked controversial cases across the country where the FBI has hacked into people's computers to discover their identity. Few defendants who had their computers hacked pursuant to a trans-jurisdictional warrant were successful in suppressing the fruits of that search, but those who were successful argued that their Fourth Amendment rights to be free from an unreasonable search and seizure were violated.

Some groups, such as the ACLU and Google, have voiced concern over the changes to Rule 41, arguing that the new rule changes the constitutional contours of the Fourth Amendment.[4] However, these fears are in many ways unfounded. To understand how the changes to Rule 41 will be interpreted in future cases, this Note will examine the series of cases concerning the trans-jurisdictional warrants which were executed before Rule 41 took effect on

[*] J.D. Candidate, May 2018, Louis D. Brandeis School of Law, University of Louisville.

[1] United States v. Levin, 186 F. Supp. 3d 26, 28–29 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017).

[2] *Id.* at 44.

[3] FED. R. CRIM. P. 41.

[4] *See* Memorandum from the Am. Civil Liberties Union to Members of the Advisory Comm. on Criminal Rules (Apr. 4, 2014) (https://www.aclu.org/other/aclu-comments-proposed-amendment-rule-41?redirect=aclu-comments-proposed-amendment-rule-41) [hereinafter Memorandum from the ACLU]; Memorandum from Richard Salgado, Google Inc., to the Judicial Conference Advisory Comm. on Criminal Rules (Feb. 13, 2015) (https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0029) [hereinafter Memorandum from Google].

December 31, 2016. In doing so, this Note will predict the future effect of the application of trans-jurisdictional warrants issued in pursuit of revealing the identity of cyber criminals. The change to Rule 41 has produced some troubling cases in its wake, but it is this Note's contention that the substantive contours of the Fourth Amendment remain unchanged. The evolution of Fourth Amendment jurisprudence is both necessary and, in this instance, does not affect the substantive rights of citizens.

In setting the backdrop around this issue, Section II will also examine the changes to Rule 41(b)(6), which allows for the issuance of warrants across jurisdictions for individuals that conceal their identity through technological means. Section II of this Note will also examine the cases of defendants like Levin, who attempted to suppress evidence obtained after the FBI installed software on their computer that revealed the IP and MAC address of their computer, thereby unmasking them. Section III will provide an analysis of the issues presented by the Network Investigative Technique (NIT) and the changes to Rule 41. Next, Section IV will propose a resolution for those issues and how courts should handle cases in which Rule 41(b)(6) is used to remotely hack into a person's computer.

Rule 41(b)(6) is also being amended to allow courts to issue warrants trans-jurisdictionally for computers suspected of being in a "botnet," but that analysis is beyond the purview of this Note. This Note also does not analyze the potential international concerns of a computer outside of the United States being searched by law enforcement for accessing suspect content which triggered a search of the computer.

II. THE "NETWORK INVESTIGATIVE TECHNIQUE" CASES

A. History of Network Investigative Techniques and Tor

In February 2015, FBI agents seized the servers of the child pornography website Playpen, which had almost 215,000 registered users and an average of 11,000 unique visitors monthly.[5] Instead of shutting down the website, the FBI allowed the website to operate normally for two weeks in order to track its users.[6] Playpen operated on an anonymous network called "The Onion Router" (Tor), and in order to track the users, the FBI obtained warrants from

[5] Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, MOTHERBOARD (Jan. 5, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

[6] *Id.*

a magistrate judge in the Eastern District of Virginia to utilize a Network Investigative Technique (NIT) and hack computers which accessed the website.[7] The NIT sent communications to the user's computer through the compromised Playpen server, causing the user's computer to transmit identifying data to the FBI.[8] In total, this warrant from the Eastern District of Virginia was used to uncover about 1,300 IP addresses, and over 1,500 cases have resulted from this FBI investigation.[9] Alex Levin was one of the people unmasked and prosecuted as a result of the seizure and monitoring of the Playpen server, and Alex Levin was one of the few to walk away from the case by suppressing the incriminating evidence found on his computer. Yet, to understand why the court in *United States v. Levin* chose to suppress the evidence obtained by the NIT, it is important to understand how Tor operates and why the FBI used the NIT.

The beginnings of Tor reach back to 1995 when the U.S. Navy Office of Naval Research sponsored researchers to develop a mechanism to anonymously communicate over the internet.[10] In 1997, the United States Department of Defense Advanced Research Projects Agency (DARPA) funded the research, and in 1998 a prototype was developed which used the basics of onion routing to create a secure network.[11] In onion routing, the purpose is to protect both the data and the identities of the parties sending and receiving that data.[12] Originally, data was sent through the onion routing network with a series of encryption keys, and each router would decrypt a layer of the data until the data reached its destination.[13] In the reverse, data is sent through the onion router network and receives a layer of encryption with each node the data passes through until it reaches its destination.[14] These layers of encryption and decryption ensure that traffic sent to target servers would appear as originating from the last onion router, or exit node.[15]

Through successive advancements which increased security and practicality in onion routers, the third generation of Tor was developed in

[7] *See id.*; *see also Levin*, 186 F. Supp. 3d at 30.

[8] *Case Study: Encryption Technology*, 10 NO. 11 QUINLAN, COMPUTER CRIME AND TECH. IN L. ENFORCEMENT, Nov. 2014.

[9] Mary-Ann Russon, *FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web*, INT'L BUS. TIMES (Jan. 6, 2016, 5:49 PM), http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417.

[10] Ramzi A. Haraty & Bassam Zantout, *The TOR Data Communication System*, 16 J. OF COMM. & NETWORKS 415, 415 (2014).

[11] *Id.*

[12] *Id.* at 416.

[13] Michael Owen, *Fun with Onion Routing*, NETWORK SECURITY, Apr. 2007, at 8–9.

[14] *Id.*

[15] Danny Bradbury, *Unveiling the Dark Web*, NETWORK SECURITY, Apr. 2014, at 14.

2004 based on the same principles developed roughly twenty years earlier.[16] In the third generation of Tor, the network can be used to access "hidden services" online.[17] These services end with the suffix ".onion," and the Tor network is designed to ensure the anonymity of both the client and the server hosting the hidden service.[18] Coupled with the rise of Bitcoin,[19] the anonymity between client and server on the Tor network allowed for the underground marketplaces to flourish.[20] One of the most notorious examples of an underground marketplace on Tor is the now defunct Silk Road, which allowed users the ability to connect and purchase goods and services ranging from drugs, fake documentation, hacking tools, and hitmen for hire.[21]

However, not all of the activity which takes place on Tor is nefarious. Tor is also used by victims of domestic violence who want to securely communicate outside the observation of their abusers, and by political dissidents in China who want to communicate freely and use websites such as Twitter.[22] Recently, Tor was instrumental in the organization of the Arab Spring of 2011, and continues to be a tool used by journalists and human-rights activists in areas like Syria.[23] Some lawyers are even using Tor to connect with clients to ensure that their communications remain privileged.[24] Tor's popularity has risen in recent years, hovering around 2 million daily connecting users,[25] and part of its popularity has been attributed to Edward Snowden's revelations about the NSA.[26]

While Tor may have several advantages, the proclivity of its users to engage in illicit activity, such as viewing and disseminating child

[16] Owen, *supra* note 13, at 9.

[17] Bradbury, *supra* note 15, at 14.

[18] *Id.*

[19] *See* Christina Rexrode, *Bitcoin Basics: What You Need to Know*, MARKET WATCH (Apr. 9, 2014, 12:01 AM), http://www.marketwatch.com/story/bitcoin-basics-what-you-need-to-know-2014-04-09 (discussing the basic background of Bitcoin).

[20] *See* Bradbury, *supra* note 15, at 15.

[21] *Id.*; Tim Hume, *How FBI Caught Ross Ulbricht, Alleged Creator of Criminal Marketplace Silk Road*, CNN (Oct. 5, 2013, 11:10 AM), http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht (discussing some of the uses of the online marketplace Silk Road).

[22] Robert W. Gehl, *Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network*, 18(7) NEW MEDIA & SOC'Y 1219, 1223 (2016).

[23] *Id.*; *see also Going Dark: The Internet Behind the Internet*, NPR (May 25, 2014, 6:54 PM), http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet.

[24] *See* Lisa Needham, *Tor Lets You Surf Anonymously and Protect Your Clients*, LAWYERIST (Nov. 11, 2014), https://lawyerist.com/78289/tor-lets-surf-anonymously-protect-clients.

[25] *Daily Connecting Users*, TORMETRICS, https://metrics.torproject.org/userstats-relay-country.html?start=2010-06-15&end=2016-09-13&country=all&events=off (last visited Feb. 12, 2017).

[26] Gehl, *supra* note 22, at 1223.

pornography, is disturbing.[27] Since information running through Tor is difficult, if not impossible, to track on its own, the FBI and other law enforcement agencies have been exploiting both human and technical weaknesses in the network to stop illegal activity.[28] Human vulnerabilities led to the takedown of the Silk Road in 2013, and in 2013 the FBI was able to seize control of the network's most prominent web host, Freedom Hosting.[29] Freedom Hosting serviced a large number of illicit websites as well as a few benign ones, such as TorMail—an anonymous email service used by political dissidents, criminals, and journalists.[30]

Due to technical limitations, tracking down individual users conducting illegal activity on Tor is challenging. Instead, the FBI has developed the NIT to identify users who are accessing websites containing illicit material. While the FBI used the NIT to identify Tor users when it seized control of the sites operated by Freedom Hosting,[31] the Bureau has also used this technique to prosecute those using Tor to access child pornography.[32]

B. Changes to Federal Rules of Criminal Procedure 41(b)

Previously, the Federal Rules of Criminal Procedure only allowed magistrate judges to issue warrants in five different scenarios. In pertinent part, the previous rule stated:

> **Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
> a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
> a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property

[27] *See* Keith Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, 11 WASH. U. GLOBAL STUD. L. REV. 715, 723 (2012) (noting the prevalence of child pornography on the Tor Network).

[28] *See* Bradbury, *supra* note 15, at 16.

[29] *See* Joshua Kopstein, *How the eBay of Illegal Drugs Came Undone*, NEW YORKER (Oct. 3, 2013), http://www.newyorker.com/tech/elements/how-the-ebay-of-illegal-drugs-came-undone.

[30] *See id.*; *see also* Meghan Neal, *The FBI Is Using Its Stash of Secure Tor Emails to Hunt Criminals*, MOTHERBOARD (Jan. 27, 2014, 11:00 AM), https://motherboard.vice.com/en_us/article/ypwg5x/the-fbi-is-using-its-stash-of-secure-tor-emails-to-hunt-criminals.

[31] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), https://www.wired.com/2013/09/freedom-hosting-fbi.

[32] *See* Brian Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 316–17 (2015).

> is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
> a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
> 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; and
> a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
> a United States territory, possession, or commonwealth;
> the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
> a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.[33]

These rules limited the authority of magistrate judges to issue warrants outside of their jurisdiction only pursuant to the investigation of domestic or international terrorism, in which activities related to the terrorism may have occurred in the issuing magistrate judge's district.[34] However, this standard became increasingly unworkable. Technological advances have made knowledge of the location of a crime increasingly difficult to ascertain because the use of software, such as Tor, masks the identity of computers used to commit crimes within the United States.[35]

C. The Application of the Previous Version of Rule 41(b) Regarding NIT Warrants

District court cases springing from the issuance of the NITs after the takedown of Playpen, a website hosting child pornography, produced a medley of results. In *Levin*, *United States v. Workman*, *United States v. Arterbury*, and *United States v. Croghan*, district courts suppressed evidence of child pornography found on the defendants' computers because the

[33] FED. R. CRIM. P. 41(b).
[34] FED. R. CRIM. P. 41(b)(3).
[35] *See* United States v. Werdene, 188 F. Supp. 3d 431, 435 (E.D. Pa. 2016).

warrants issued out of the Eastern District of Virginia by the magistrate judge were invalid *ab initio*, or at issuance.[36] However, the majority of courts reviewing suppression motions regarding the NIT warrants issued out of the Eastern District of Virginia did not find suppression appropriate.[37] Though the majority of district courts denied the motion to suppress, their reasons for doing so were varied.[38] While much of the disparate reasoning employed by district courts are now obsolete due to the change in Rule 41, several district court holdings are still applicable after the change. A discussion of the analysis employed by district courts analyzing suppression motions regarding the NIT warrants illuminates the implications of some of the district court holdings on future cases concerning revised Rule 41 and the Fourth Amendment.

In evaluating motions to suppress NIT warrants, district courts generally employed a similar analysis. First, several courts discussed whether there was a privacy interest in the information collected by the NIT.[39] Second, courts analyzed whether the warrant was issued with probable cause and particularity in accordance with Fourth Amendment requirements.[40] Third, courts discussed whether the magistrate judge exceeded her authority under the 28 USC § 636(a) by issuing the NIT pursuant to Rule 41(b).[41] Fourth, if there was a violation, courts addressed whether that violation was substantive or technical.[42] If the violation was technical, courts analyzed whether the violation was prejudicial or deliberate.[43] Finally, if the violation was prejudicial or deliberate as a technical violation, or a substantive constitutional violation, then courts determined whether the good-faith

[36] *See* United States v. Levin, 186 F. Supp. 3d 26, 35, 44 (2016), *vacated*, 874 F.3d 316 (1st Cir. 2017); United States v. Workman, 205 F. Supp. 3d 1256, 1259, 1267 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *34-35 (N.D. Okla. April 25, 2016); United States v. Croghan, 209 F. Supp. 3d 1080, 1091, 1093 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018).

[37] *See, e.g.*, United States v. Broy, 209 F. Supp. 3d 1045, 1048 (C.D. Ill. 2016); United States v. Darby, 190 F. Supp. 3d 520, 523 (E.D. Va. 2016); *Werdene*, 188 F. Supp. 3d at 436.

[38] *Compare* United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016) (suppression was inappropriate because the NIT warrant was authorized under Fed. R. Crim. P. 41(b)(4); the NIT was akin to a tracking device), *with Broy*, 209 F. Supp. 3d at 1054-55, 1057 (holding Fed. R. Crim. P. 41 was violated and the warrant was void *ab initio*; the good-faith exception applied).

[39] *See* United States v. Darby, 190 F. Supp. 3d 520, 528 (E.D. Va. 2016); *Matish*, 193 F. Supp. 3d at 615.

[40] *See Broy*, 209 F. Supp. 3d at 1050; *Matish*, 193 F. Supp. 3d at 602.

[41] *See* United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *5 (M.D. Fla. Aug. 10, 2016); *Werdene*, 188 F. Supp. 3d at 440.

[42] *See, e.g.*, *Levin*, 186 F. Supp. 3d at 35.

[43] *See Werdene*, 188 F. Supp. 3d at 446.

exception applies to the law enforcement officials' actions in applying for the warrant.[44]

1. Privacy in the Searched Computer or in the Acquired Data

As an introductory matter, several courts analyzed whether the defendants in the NIT cases had a privacy right to their IP addresses, which was used to track the users who accessed the Playpen site. In doing so, the majority of courts determined that the defendants did have a Fourth Amendment privacy interest in their computers, which the FBI bugged in order to determine the IP addresses of the accessing computers.[45] However, a minority of courts reasoned that the defendants had no expectations of privacy in their IP addresses, and therefore no warrants were needed to conduct the search of their computers to access their IP addresses.[46]

To determine whether Fourth Amendment protections apply, the Supreme Court in *Smith v. Maryland* held that the query "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 government action."[47] This analysis turns on whether the individual "exhibited an actual (subjective) expectation of privacy;" and whether the expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[48] In determining whether there is an expectation of privacy in an IP address, the United States argued in the NIT cases that because *Smith* held there was no expectation of privacy in the phone numbers individuals dial due to the fact that they voluntarily give that information to third-party phone companies, then there should be no expectation of privacy in IP addresses because Tor users convey that information to third-party nodes before entering the Tor network.[49] Therefore, some district courts reasoned, since there is no expectation of privacy in an IP address, the FBI did not conduct a search by implementing the NIT.[50] Moreover, several courts have held that there is no expectation of privacy in an IP address because internet users convey that information to third-party servers on the internet.[51]

[44] *See, e.g.*, *Levin*, 186 F. Supp. 3d at 38.

[45] *See, e.g.*, *Darby*, 190 F. Supp. 3d at 530.

[46] *See Werdene*, 188 F. Supp. 3d at 436; United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *5 (N.D. Cal. Sept. 1, 2016).

[47] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[48] *Id.* (citations omitted).

[49] *Darby*, 190 F. Supp. 3d at 530 (citing *Smith*, 442 U.S. at 745).

[50] *See id.*

[51] *See* United States v. Caira, 833 F.3d 803, 806 (7th Cir. 2016); United States v. Christie, 624 F.3d

In *United States v. Matish,* however, the court went further, stating that the prevalence of hacking is changing the public's reasonable expectation of privacy on their computer.[52] The court then lists, in uncomfortable detail, the prevalence of hacking in our society: from Apple's failure to prevent iPhones from being unlocked, to the Ashley Madison hacks, to Home Depot's 56 million credit card hack, and so on.[53] In essence, unencrypted data on the internet is free to be viewed and tampered; in the same way that regular internet users cannot reasonably expect to be safe from hackers, neither can Tor users.[54]

Because of the ubiquity of hacking, the *Matish* court reasoned that "hacking resembles the broken blinds in *Carter.*"[55] Moreover, "[j]ust as Justice Breyer wrote in concurrence that a police officer who peers through broken blinds does not violate anyone's Fourth Amendment rights. . . FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment."[56] However, other courts, such as *United States v. Werdene,* which held the NIT was not a search within the meaning of the Fourth Amendment, stop their subjective expectation of privacy analysis upon concluding that there is no expectation of privacy in an IP address.[57]

Conversely, other courts, such as *United States v. Broy,* reason that there is an expectation of privacy in a computer,[58] and therefore conclude the NIT constituted a Fourth Amendment search.[59] In making this determination, the *Broy* court relied upon *California v. Riley,* in which the Supreme Court rejected the notion that police officers may search a cell phone in order to access the call log.[60] The defendant in *Riley* had a legitimate expectation of privacy in his phone regardless of whether or not there was an expectation of privacy in some of the data on his phone.[61] *United States v. Darby* made a similar holding, concluding that, "the 'contents' of a computer are nothing but code," and that "[i]n placing code on the Defendant's computer, the government literally—one writes code—invaded the contents of the computer."[62] Therefore, even if Darby did not have an expectation of privacy

558, 574 (3d Cir. 2010); United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008).

[52] *Matish,* 193 F. Supp. 3d at 619–20.

[53] *Id.*

[54] *Id.* at 620.

[55] *Id.* (citing Minnesota v. Carter, 525 U.S. 83, 85 (1998)).

[56] *Id.* (citing *Carter,* 525 U.S. at 103).

[57] *See, e.g.,* United States v. Werdene, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016).

[58] United States v. Broy, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016).

[59] *Id.* at 1055.

[60] *Id.* at 1054; *see also* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014).

[61] *Riley,* 134 S. Ct at 2492–93.

[62] United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016).

in his IP address, he did have an expectation of privacy in his computer, which the government bugged in order to obtain his IP address.[63] Therefore, according to *Darby*, the NIT was a Fourth Amendment search.[64]

2. Probable Cause to Issue the NIT

Next, the NIT cases analyzed whether there was probable cause to conduct the search and whether there was sufficient particularity to satisfy Fourth Amendment requirements. Notably, none of the courts that have touched on this issue held that there was insufficient probable cause or particularity in the NIT warrant.[65]

The Fourth Amendment provides:

> 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 particularity describing the place to be searched, and the persons or things to be seized.[66]

Probable cause provides deference to the magistrate issuing the warrant, requiring only that the magistrate "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place."[67] In reviewing a determination of probable cause, the "reviewing court is simply to ensure that the magistrate had a substantial basis for. . . conclude[ing] that probable cause existed."[68]

The reasoning set forth in *Matish* is typical of the reasoning set forth in other cases handling probable cause regarding the NIT warrants. In *Matish*, the court held that there was sufficient probable cause to issue the warrant because the affidavit detailed that: the website Playpen was almost completely comprised of child pornography and child abuse; users had to

[63] *Id.*

[64] *Id.* Other courts have used similar reasoning. *See, e.g.*, *Broy*, 209 F. Supp. 3d at 1053.

[65] *See Darby*, 190 F. Supp. 3d at 532 (finding both particularity and probable cause for issuing the NIT warrant); *Broy*, 209 F. Supp. 3d at 1051 (finding sufficient particularity); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 15, 2016) (finding sufficient probable cause); United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *8 (W.D. Wash. Jan. 28, 2016) (finding both particularity and probable cause).

[66] U.S. CONST. amend. IV.

[67] Illinois v. Gates, 462 U.S. 213, 238 (1983).

[68] *Id.* at 238–39.

deliberately register to the site to access it; the logo contained sexually suggestive prepubescent children; and the nature of Tor's structure makes it difficult to accidentally stumble upon hidden services without directly seeking them out.[69] Therefore, the *Matish* court concluded that there existed sufficient probable cause for the magistrate to issue the NIT warrant.[70]

The Fourth Amendment also requires that the search warrant particularly describe "the place to be searched, and the persons or things to be seized."[71] Particularity limits the authorization of the search "to the specific areas and things for which there is probable cause to search" and "ensures that the search will be carefully tailored to is jurisdictions, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[72] Particularity is satisfied with regard to place if "the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended."[73] Furthermore, particularity is satisfied with the things to be seized when "nothing [is] left to the discretion of the officer executing the warrant."[74] With regard to the NIT warrant, in *Broy*, the court reasoned the warrant was sufficiently particular both because the warrant described that it would only deploy on activating computers which affirmatively logged into Playpen, wherever located, and because the NIT warrant limited its data collection to specific, necessary information, the most important of which was the IP addresses.[75]

3. Magistrate Authority

Next, the cases discuss whether the issuance of the NIT warrant exceeded the magistrate's authority under 28 USC § 636(a) by issuing the warrant

[69] United States v. Matish, 193 F. Supp. 3d 585, 603–04 (E.D. Va. 2016).

[70] *Id.* at 604.

[71] U.S. CONST. amend. IV.

[72] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[73] Steele v. United States, 267 U.S. 498, 503 (1925).

[74] Marron v. United States, 275 U.S. 192, 196 (1927).

[75] United States v. Broy, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016). The particular information seized by the NIT warrant included: 1) the 'activating' computer's actual IP address, and the date and time that the NIT determines what that IP address is; 2) a unique identifier generating by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other 'activating' computers, that will be sent with and collected by the NIT; 3) the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); 4) information about whether the NIT has already been delivered to the 'activating' computer; 5) the 'activating' computer's Host Name; 6) the 'activating' computer's active operating system username; and 7) the 'activating' computer's media access control ('MAC') address. United States v. Levin, 186 F. Supp. 3d 26, 30 n.5 (D. Mass. 2016).

pursuant to Rule 41(b).[76] As much of the conflicting rulings in this area are now moot due to the changes in the Rule 41(b), this section will only detail some of the holdings that may have enduring impact. While most courts' rulings on suppression motions regarding NIT warrants either assumed or found that the warrants violated Rule 41(b),[77] a minority of jurisdictions found the warrants permissible under Rule 41(b)(4) as they ruled the NIT was akin to a tracking device.[78]

Rule 41(b)(4) authorizes a magistrate to issue a warrant to install within the district a tracking device which would track the movement of a person or property located within the district, outside the district, or both.[79] The three cases which found that the NIT warrant was authorized under Rule 41(b)(4) all assume that the defendants' property traveled to the Eastern District of Virginia, where the FBI was hosting the Playpen server, thereby allowing the government to install a "tracking device" on their data, which then followed the data back to the defendants' computers in their respective districts.[80]

In *United States v. Jean*, the court justified the warrant under Rule 41(b)(4) by parsing out the language of Rule 41(b)(4) and applying it to the NIT. First, the *Jean* court determined that the NIT was an "electronic device" under 18 U.S.C. § 3117(b) "because it is an investigative tool consisting of computer code transmitted electronically over the internet."[81] Next, the NIT tracked the movement of "property," which includes "information" per the definition of "property" in Rule 41(a)(2)(A).[82] The *Jean* court further asserted that the NIT was "installed" in the Eastern District of Virginia.[83] This leap is made by urging that the defendant's electronic data, traveling in search of illicit material, caused a string of computer code to be executed and deployed

[76] *See* United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *5 (M.D. Fla. Aug. 10, 2016); United States v. Werdene, 188 F. Supp. 3d 431, 440 (E.D. Pa. 2016).

[77] *See Werdene*, 188 F. Supp. 3d at 442; United States v. Croghan, 209 F. Supp. 3d 1080, 1089 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018); United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *6 (W.D. Tex. Sept. 9, 2016); United States v. Workman, 205 F. Supp. 3d 1256, 1261 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018); United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at * 3 (N.D. Cal. Sept. 1, 2016).

[78] *See* United States v. Austin, 230 F. Supp. 3d 828, 832–33 (M.D. Tenn. 2017); United States v. Jean, 207 F. Supp. 3d 920, 937–38 (W.D. Ark. 2016); United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *6 (D. Neb. Aug. 5, 2016).

[79] FED. R. CRIM. P. 41(b)(4).

[80] *See* United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016); United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *6 (W.D. Mo. Oct. 20, 2016); United States v. Jean, 207 F. Supp. 3d 920, 942–43 (W.D. Ark. 2016).

[81] *Jean*, 207 F. Supp. 3d at 942.

[82] *Id.*

[83] *Id.*

from the Eastern District of Virginia to his computer in the Western District of Arkansas.[84] To hold otherwise, the court reasoned, "would require finding that magistrate judges do not currently possess authority to issue information-tracking warrants; but such a reading is squarely contradicted by the plain language of Rule 41(a)(2)(A)."[85]

4. Rule 41(b) Violation as Constitutional or Technical

If the court assumed or concluded that a violation of Rule 41(b) occurred, then in the next step of the analysis the court determined whether the violation was constitutional/substantive, or ministerial/technical.[86] The majority of courts held that the violation is technical.[87] Similar to other courts, the *United States v. Adams* court found that the violation of Rule 41(b) was technical because the Fourth Amendment does not impose a venue requirement, but only requires that "(1) a search warrant must be issued by a neutral magistrate; (2) it must be based on a showing of probable cause, and (3) it must satisfy the particularity requirement."[88] Since none of the courts found the NIT warrant void of probable cause or particularity,[89] many found the violation, if there was one, merely technical or ministerial.[90]

However, other courts viewed the violation as constitutional or substantive.[91] In *Broy*, the court concluded that "because the warrant was issued without lawful authority under Rule 41, it [was] void at the outset, or *ab initio*."[92] The Western District of Kentucky made a similar ruling, reasoning that because the issuing magistrate "had no jurisdiction or authority under the Federal Magistrates Act to issue the NIT warrant, the Court holds

[84] *Id.* at 943.

[85] *Id.*

[86] *Compare* United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *1 (N.D. Cal. Sept. 1, 2016) (holding that the Rule 41 violation was technical, not substantive), *with* United States v. Levin, 186 F. Supp. 3d 26,36 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017) (holding that the Rule 41 violation was substantive, not ministerial).

[87] *See* United States v. Werdene, 188 F. Supp. 3d 431, 447 (E.D. Pa. 2016); Henderson, 2016 WL 4549108, at *1; United States v. Torrees, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *7 (W.D. Tex. Sept. 9, 2016); United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016).

[88] *Adams*, 2016 WL 4212079, at *7 (citing Dalia v. United States, 441 U.S. 238, 255 (1979)).

[89] *See supra* note 65.

[90] *See supra* note 86.

[91] *See* United States v. Levin, 186 F. Supp. 3d 26, 36 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017); United States v. Broy, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016); United States v. Ammons, 207 F. Supp. 3d 731, 741–42 (W.D. Ky. 2016).

[92] *Broy*, 209 F. Supp. 3d at 742 (citation and quotation marks omitted).

that the NIT warrant was void from the beginning (or *ab* initio, in Latin)."[93] *Levin* contends that Rule 41 has both procedural and substantive requirements, but that Rule 41(b) "is a substantive provision" because the "violation at issue here. . . involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant."[94] Therefore, because the warrant was void *ab initio*, it is treated as if there were no warrant at all, meaning that the government NIT search violated the defendant's Fourth Amendment constitutional rights.[95]

5. Prejudice and the Good-Faith Exception

The next step in the analysis—for courts which held any Rule 41(b) violation was technical—is to determine whether the violation was prejudicial to the defendant or constituted deliberate disregard of the Rule.[96] Courts differ on how to define prejudice, with the Tenth Circuit in *United States v. Krueger* regarding prejudice "in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed,"[97] and the Third Circuit in *United States v. Cox* defining prejudice "in the sense that it offends concepts of fundamental fairness or due process."[98] In *Adams*, the court, following a similar definition of prejudice given in *Krueger*,[99] reasoned that prejudice occurred because the "law enforcement had no realistic chance of identifying the IP address associated with Defendant's computer without the NIT."[100] Based on this premise, the court reasoned that "[h]ad the magistrate judge followed Rule 41(b), the search of Defendant's computer would not have occurred."[101] However, in

[93] *Ammons*, 207 F. Supp. 3d at 742; *see also* United States v. Master, 614 F.3d 236, 239 (6th Cir. 2010).

[94] *Levin*, 186 F. Supp. 3d at 35 (citing United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008)). For the proposition that Rule 41(b) is substantive, see United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) "implicates substantive judicial authority"), and United States v. Glover, 736 F.3d 509, 515 (D.C. Cir.2013) (holding that violation of Rule 41(b) is a jurisdictional flaw and not a technical violation).

[95] *See Ammons*, 207 F. Supp. 3d at 742; United States v. Workman, 205 F. Supp. 3d 1256, 1266–67 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018).

[96] *See* United States v. Werdene, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016); United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016).

[97] United States v. Krueger, 809 F.3d 1109, 1115 (10th Cir. 2015).

[98] United States v. Cox, 553 Fed. Appx. 123, 128 (3d Cir. 2014).

[99] The exact definition of prejudice in this instance comes from United States v. Loyd, 721 F.2d 331, 333 (11th Cir. 1983) (stating suppression of the evidence is necessary "only where (1) there [is] 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed").

[100] *Adams*, 2016 WL 4212079, at *8.

[101] *Id.*

Jean, the defendant failed to show prejudice because "an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant," which would have led to the defendant's subsequent arrest.[102]

In respect to suppressing the evidence due to the deliberate disregard of the Rule, the majority of courts dismissed this notion by noting the conflicting case law could show "at least a good-faith basis existed to allow the officers to believe the warrant satisfied Rule 41(b)(4)."[103] None of the courts finding the Rule 41(b) violation technical found the FBI officers acted in deliberate disregard of the rule. However, this may be because the good-faith exception analysis subsumes this discussion.

Finally, if the violation was prejudicial or deliberate as a technical violation, or a substantive constitutional violation, then courts determined whether the good-faith exception applied to the law enforcement officials' actions in applying for the warrant.[104] In general, suppression is considered a "last resort, not [a] first impulse."[105] Moreover, excluding evidence is not a defendant's individual right, but is only applicable as a deterrent for future Fourth Amendment violations.[106] The Supreme Court has explained that "[e]ach time the exclusionary rule is applied it exacts a substantial societal cost for the vindication of the Fourth Amendment rights,"[107] and that this deterrent value must outweigh the "substantial societal costs."[108] The deterrent value can outweigh the costs "[w]hen the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights.[109] However, "[w]hen the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful," then there is little deterrent value and exclusion is not the appropriate remedy.[110]

The majority of courts discussing the NIT warrants have held that, if there were any Fourth Amendment violation, the good-faith exception to exclusion applies.[111] The courts in *Broy* and *United States v, Ammons* held

[102] United States v. Jean, 207 F. Supp. 3d 920, 944 (W.D. Ark. 2016).

[103] *Id.*; *see also* United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *6 (N.D. Cal. Sept. 1, 2016).

[104] *See* United States v. Croghan, 209 F. Supp. 3d 1080, 1091 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018).

[105] Hudson v. Michigan, 547 U.S. 586, 591 (2006).

[106] Herring v. United States, 555 U.S. 135, 141 (2009) (citing United States v. Leon, 468 U.S. 897 (1984)).

[107] Rakas v. Illinois, 439 U.S. 128, 137 (1978).

[108] United States v. Leon, 468 U.S. 897, 909 (1984).

[109] Davis v. United States, 564 U.S. 229, 238 (citing *Herring*, 555 U.S. at 144).

[110] *Id.* (citing *Leon*, 468 U.S. at 909).

[111] *See* United States v. Broy, 209 F. Supp. 3d 1045, 1057–58 (C.D. Ill. 2016); United States v. Ammons, 207 F. Supp. 3d 732, 743–44 (W.D. Ky. 2016).

that even if the warrant was void *ab initio*, the good-faith exception to exclusion still applies.[112] This reasoning is founded in the balancing test discussed in *Herring v. United States*, which compares the deliberate and culpable actions of the police against exclusion's deterrent value.[113] Moreover, *Ammons* relied on the Sixth Circuit's determination in *United States v. Master* in ruling that "[t]he good-faith exception to the exclusionary rule is not foreclosed in situations where a warrant is void *ab initio*."[114] The *Ammons* court further reasoned that the legal status of the warrant "merely informs, but does not control, the Court's good-faith analysis."[115] Applying this reasoning, *Ammons* and *Broy* concluded that the FBI's exceedingly detailed application for the warrant, and the subsequent issuing of the warrant, evidenced its objectively reasonable good faith in relying on the NIT warrant.[116] Furthermore, both courts found that the only deterrent value is in deterring the magistrate's actions in issuing the warrant, which is outside the scope of the good-faith exception to exclusion analysis.[117]

Other cases holding that the NIT warrant was void *ab initio* come to a different conclusion, which is that the good-faith exception does not apply to warrants void *ab initio*.[118] In concluding thus, the *Levin* court premised that "a warrant that was void at the outset is akin to no warrant at all."[119] For support, *Levin* looked to the First Circuit, which "declined to 'recognize[] a good-faith exception in respect to warrantless searches."[120] According to *Levin*, the distinction between a voidable and a void warrant is significant because the former is premised on "statutory requirements" while the latter is premised on "judicial authority."[121] Therefore, to maintain the distinction between a voidable and a void warrant, the court in *Levin* declined to find the

[112] *Id.*

[113] *Herring*, 555 U.S. at 144.

[114] *Ammons*, 207 F. Supp. 3d at 744; *see also* United States v. Master, 614 F.3d 236, 241–43 (6th Cir. 2010).

[115] *Ammons*, 207 F. Supp. 3d at 744.

[116] *Id.* at 744–45; *Broy*, 209 F. Supp. 3d at 1058.

[117] *See Ammons*, 207 F. Supp. 3d at 744–45; *Broy*, 209 F. Supp. 3d at 1058.

[118] *See* United States v. Levin, 186 F. Supp. 3d 26, 38 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017); United States v. Croghan, 209 F. Supp. 3d 1080, 1090 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018); United States v. Workman, 205 F. Supp. 3d 1256, 1266–67 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018).

[119] *Levin*, 186 F. Supp. 3d at 41.

[120] *Id.* (citing United States v. Curzi, 867 F.2d 36 (1st Cir. 1989)).

[121] *Id.* (citing State v. Hess, 770 N.W.2d 769, 775 (Ct. App. Wis. 2009)); *see also* State v. Vickers, 964 P.2d 756, 762 (Mont. 1998) ("If a search warrant is void *ab initio*, the inquiry stops and all other issues pertaining to the validity of the search warrant, such as whether the purpose of the exclusionary rule is served, are moot.").

good-faith exception applicable.[122] Moreover, the court in *Levin* determined that even if the good-faith exception did apply, "it was not objectively reasonable for law enforcement—particularly a veteran FBI agent with 19 years of federal law enforcement experience—to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b)."[123] Three other districts have been inclined to follow the *Levin* court's analysis, with two agreeing that the good-faith exception is inapplicable to warrants void *ab initio*,[124] and one agreeing that the FBI did not act in good faith seeking the warrant.[125]

D. Conclusion to History

While some issues discussed above are now moot due to the change in Rule 41(b), the cases above are still instructional because they lay the groundwork for how the Fourth Amendment will apply to searches conducted digitally through the internet and across jurisdictions.

III. HOW WILL REVISED RULE 41(B) BE APPLIED?

This section will discuss the application of Rule 41(b)(6) based on the NIT cases above. For reference, Rule 41(b)(6) reads as follows:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[126]

[122] *Id.*

[123] *Id.* at 42.

[124] *See* United States v. Workman, 205 F. Supp. 3d 1256, 1266–67 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *3 (N.D. Okla. Apr. 25, 2016).

[125] *See* United States v. Croghan, 209 F. Supp. 3d 1080, 1090–91 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018).

[126] FED. R. CRIM. P. 41(b)(6).

A. Privacy Right to Information

As the FBI becomes increasingly active in the field of cybersecurity and cracking down on illicit activity on the internet, the right to privacy of information will inevitably become a recurring theme with which courts will be forced to grapple. Rule 41(b)(6) will mitigate some of the need to delve into this analysis because properly issued warrants will vitiate the need to determine what data is private on a computer due to the government having a right to search or seize that information pursuant to Fourth Amendment requirements. However, in determining whether to seek a warrant, based on the above NIT cases in which courts held that the NIT did not obtain private information,[127] government officials may choose to forgo the procedure in favor of collecting metadata from less protected areas of the internet[128] or to hack into computers to retrieve what the government perceives to be non-private information.

Given some of the holdings in *Werdene*, *Matish*, and *United States v. Henderson*, government agents may choose not to apply for a warrant and may instead choose to bug computers to retrieve the IP address. Though this course of action will not likely stand due to the Supreme Court's holding in *Riley*—holding that police officers were foreclosed from accessing a phone without a warrant to retrieve non-private information, such as call logs[129]—these cases do raise some concerning problems. Though government officials may not be able to hack a computer in order to access non-private information, because computers often contain large amounts of private data, this does not necessarily prohibit government officials from hacking into a personal router to monitor non-private metadata.[130] Routers are not immune to hacking,[131] and since routers do not contain large amounts of personal information like a phone or a computer, and since that data is being

[127] *See* United States v. Werdene, 188 F. Supp. 3d 431, 445 (E.D. Pa. 2016).

[128] *See generally* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757, 863 (2014) (surveying metadata collection practices by the Government and discussing the Government's reliance on *Smith v. Maryland* as justification for bulk metadata collection).

[129] *See* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014).

[130] *See* Jennifer Valentino-Devries, *Rarely Patched Software Bugs in Home Routers Cripple Security*, WALL STREET J. (Jan. 18, 2016, 11:58 AM), https://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285?tesla=y; *see also* David Gilbert, *Router Hack Creates 'Ultimate Listening Device' to Monitor a Country's Entire Internet Traffic*, INT'L BUS. TIMES (Sept. 15, 2015, 12:59 PM), http://www.ibtimes.com/router-hack-creates-ultimate-listening-device-monitor-countrys-entire-internet-2097511.

[131] *See* Seth Rosenblatt, *Top Wi-Fi Routers Easy to Hack, Says Study*, CNET (Apr. 17, 2013, 11:00 AM), https://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study.

transmitted to third-party servers, there may be no legitimate expectation of privacy in a router and the non-private information that passes through it.[132] This scenario appears unlikely, however, due to the minority of courts which held that a warrant was not needed to hack into a computer to log non-private information, and due to the holding in *Riley*, recognizing an expectation of privacy in non-private information contained on a personal phone, which is analogous to a personal computer and router.[133]

B. Probable Cause and Particularity

Probable cause and particularity were not issues in the NIT cases. All of the courts addressing these issues found that there was sufficient probable cause and the warrants were sufficiently particular in describing the information to be searched and seized. While this was not an issue in these cases, as the digital age barrels on, and with approval from revised Rule 41, government officials may wish to expand their investigations.

If the FBI expands its online sting operations on Tor or elsewhere on the internet, then probable cause will become increasingly problematic for judges issuing trans-jurisdictional warrants. In the NIT cases, probable cause was clear because the site Playpen consisted almost entirely of child pornography, it existed on Tor—which is currently difficult to navigate—and the site required a login and password for access.[134] These factors sufficiently indicate that users accessing Playpen were intentionally attempting to access child pornography.

However, Tor is growing rapidly, and now over one million people use Tor to access Facebook.[135] As Tor grows and matures from a shadowy and confusing network to resemble more and more the regular internet, then the difficult navigability of Tor will cease to be a factor supporting probable cause because users would be more likely to accidentally stumble upon a site hosting illicit content.[136] Moreover, sites that host illicit material on Tor may

[132] This issue has not been addressed directly by any court. However, the Third Circuit has held that an individual has no reasonable expectation of privacy in a wireless signal transmitted over an unsecured network. United States v. Stanley, 753 F.3d 114, 115 (3d Cir. 2014); *but see* United States v. Heckenkamp, 482 F.3d 1142, 1146–48 (9th Cir. 2007) (defendant had a reasonable expectation of privacy in content shared over monitored university network, but the privacy expectation is reduced if the user is aware the transmitted information is not secure).

[133] *See* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014).

[134] *See* United States v. Darby, 190 F. Supp. 3d 520, 532 (E.D. Va. 2016).

[135] *See* Alec Muffett, *1 Million People Use Facebook Over Tor*, FACEBOOK (Apr. 22, 2016), https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648.

[136] Tor continues to rapidly grow. *See* Mary-Ann Russon, *Dark Web Mystery: 25,000 New Tor.onion*

remove username and password requirements to access the site due to the Playpen sting operation, meaning that a username and password for these illicit sites could act as a signal that the site is a honeypot designed to trap users. The FBI, in seizing and operating servers hosting illicit content, may be compelled to stop requiring logins from users if this becomes a warning sign to the internet community wishing to access this illicit data. If these two factors are removed, however, it becomes a closer determination of whether probable cause exists. A stray click may not create a fair probability that a user is engaging in a crime, especially when the consequences result in the government hacking a computer hosting large amounts of private and sensitive information.

On the other hand, particularity will not likely be an issue in future NIT cases. Based on the NIT cases, if the government only seeks warrants pertaining to specific, identifying information about the user who triggered the search by accessing the honeypot, then this sort of request is sufficiently narrow to prevent a fishing expedition by the government.[137] IP addresses and MAC addresses can be changed and spoofed,[138] so this information may not always reveal the identity of a user accessing a honeypot that then bugs their computer. Monitoring this data for a reasonable amount of time while the government acts on the search warrant can mitigate the possibility of users concealing their digital identity, but could also run afoul of the particularity requirement. Additionally, hacking a computer accessing a honeypot to transmit GPS coordinates may be permissible, but it is unlikely that warrants seeking information such as GPS coordinates and other information to spy on the user, such a webcam video, over an extended period will adhere to the particularity requirements imposed by the Fourth Amendment.[139]

Sites Have Suddenly Appeared – and Nobody Knows Why, INT'L BUS. TIMES (Feb. 22, 2016, 4:14 PM), http://www.ibtimes.co.uk/dark-web-mystery-25000-new-tor-onion-sites-have-suddenly-appeared-nobody-knows-why-1545323.

[137] *See generally In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (holding that an expansive technological search including data mining, monitoring, and tracking violated the Fourth Amendment's particularity requirement). For a definition of "honeypot," see *Honeypots: The Sweet Spot in Network Security*, COMPUTERWORLD (Nov. 20, 2003, 12:00 AM), https://www.computerworld.com/article/2573345/security0/honeypots--the-sweet-spot-in-network-security.html ("A honeypot is a system that's put on a network so it can be probed and attacked. Because the honeypot has no production value, there is no 'legitimate' use for it. This means that any interaction with the honeypot, such as a probe or scan, is by definition suspicious."). Honeypots are, in essence, a trap.

[138] *See* Jack Wallen, *How to Work with Networking Profiles in GNOME*, TECHREPUBLIC (Feb. 9, 2017, 9:04 AM), http://www.techrepublic.com/article/how-to-work-with-networking-profiles-in-gnome (discussing a benign reason to change IP addresses or spoof a MAC address).

[139] *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 759.

C. Concerns Not Related to the Fourth Amendment

Most of the analysis employed by the NIT cases regarding the Rule 41(b) violation is now moot due to the change in Rule 41(b), which negated the need to seek alternate justification for warrants which are issued trans-jurisdictionally by a magistrate judge. However, the analysis by some of the courts in attempting to justify the warrant under Rule 41 could prove problematic.

Specifically, several courts reviewing the NIT found that the warrant was valid under Rule 41(b)(4) because the NIT was akin to a tracking device.[140] To complete this analysis, the district courts were required to assume that the defendant's property traveled to the Eastern District of Virginia, wherein that property or information was installed with a tracking device which traveled back to the jurisdiction where the accessing computer resided.[141]

This reasoning does not comport with the facts of how the NIT works. The accessing computer sent a request to the Playpen server for data, and the Playpen server responded by sending requested data through the Tor nodes back to the accessing computer.[142] The accessing computer's data is not making a round trip to the server, picking up data, and traveling back to the accessing computer like a vehicle. Instead, two separate strings of data are traveling back and forth: the request from the accessing computer and the response from the server. The information sent back to the accessing computer from the server is separate from the request for information sent to the server. Therefore, since the accessing user's information is separate from the requested information from the server, the tracking device analogy necessarily fails because the requested data is not in possession of the user until received.

A proper understanding of the mechanisms in motion allow for the proper application of law. By holding that the user's property travels to various jurisdictions while on the internet in furtherance of a crime could subject a potential defendant committing crime on the internet to forum shopping.[143] Data sent to and from servers passes through multiple jurisdictions, making stops at domain name system (DNS) servers along the way to properly route the data to its destination. It is not farfetched to imagine, based on these

[140] *See* United States v. Matish, 193 F. Supp. 3d 585, 613 (E.D. Va. 2016).

[141] *Id.*

[142] *See supra* notes 13–22 and accompanying text; *see also Tor: Overview*, TOR PROJECT, https://www.torproject.org/about/overview (last visited Feb. 1, 2017) (brief overview of the basic functions of Tor).

[143] *See* Memorandum from the ACLU, *supra* note 4, at 3.

holdings, that the government may charge a defendant for a crime in the jurisdiction where the server is located because the defendant committed a crime there by accessing and retrieving illicit material.

Forum shopping may also be an issue regarding the magistrate issuing the warrant. Currently, Rule 41(b)(6) allows a magistrate judge to issue the warrant "in any district where activities related to a crime may have occurred."[144] This broad, sweeping language may encourage law enforcement officials to seek a favorable jurisdiction when seeking warrants because of the borderless nature of the internet and the difficulty of knowing where internet users are when they are perpetuating crimes. However, this provision appears necessary given the need to update the Federal Rules of Criminal Procedure and allow for the FBI to more effectively combat cybercrime.

Overall, these changes in Rule 41 were necessary in order to fix the glaring venue problems that cybercrimes caused for law enforcement and the courts. While groups such as the ACLU and companies such as Google have voiced concerns over the Rule 41 expansion,[145] ultimately the amendment does not alter Fourth Amendment principles. How these principles are used to fit the nature of cybercrime within that framework is a difficult matter and has produced curious results, but the expansion of Rule 41(b) does not tread upon Fourth Amendment rights, it merely allows magistrate judges to apply those principles to an expanded digital realm.

IV. RESOLUTION

In the coming years, as Tor expands or other encryption technologies which conceal the identity of cyber criminals emerge, it is important for both the government to combat illicit activity and for individuals to be free from intrusive actions by the government into their personal and digital spheres. If magistrate judges familiarize themselves with the proper technological mechanisms regarding the warrants they issue, then strange outcomes, such as courts holding that defendants are traveling to various jurisdictions when accessing servers, are unlikely to occur. Moreover, magistrate judges familiar with the technological processes of potential warrants will better understand any probable cause and particularity issues. Detailed affidavits by the government, like the ones in the NIT cases,[146] are crucial to ensuring the

[144] FED. R. CRIM. P. 41(b)(6).

[145] *See* Memorandum from the ACLU, *supra* note 4, at 3; *see also* Memorandum from Google, *supra* note 4.

[146] *See* United States v. Matish, 193 F. Supp. 3d 585, 594–95 (E.D. Va. 2016).

correct decision is made before a warrant is issued due to the difficulty of suppressing ill-gotten evidence.

A. Forum Shopping

Forum shopping concerns are legitimate, as Rule 41 states that a magistrate judge may issue a warrant to search computers in "any district where activities related to a crime may have occurred."[147] This broad language could encompass potentially every district in the United States given the way data is transferred and stored on the internet. It is likely that, as in the NIT cases above, the FBI will ask for warrants in the jurisdiction in which they set up the honeypot server to trap users attempting to access illicit content. Rule 41 does not expand where a defendant may be charged or tried as the same concerns which could lead to forum shopping in the indicting venue—that internet crimes can be interpreted as occurring in several jurisdictions simultaneously—are additionally present for all cybercrimes. Ideally, however, forum shopping is best combatted by restricting the prosecution of cybercrimes to the venue where the accessing computer is located.

B. Magistrate Shopping

The recent amendment to Rule 41 could implicate magistrate shopping, which constitutes a Fourth Amendment violation if the claim challenges a magistrate's neutrality.[148] Magistrate shopping can occur when the FBI or other authorities specifically seek warrants in favorable jurisdictions where judicial discretion concerning probable cause is more lenient. Excluding evidence based on magistrate shopping is only an issue when there is already a probable cause defect in the warrant application,[149] and ultimately still requires bad faith on the part of the applying officer.[150] Since Rule 41 does not expand probable cause or particularity requirements—it instead invites judicial application of probable cause and particularity requirements to an expanded area of the law—then the changes to Rule 41 should only cause limited concern for magistrate shopping.

Law enforcement agents may be able to shop for magistrates willing to grant warrants seeking to comb through information on a person's computer.

[147] FED. R. CRIM. P. 41(b)(6).

[148] *See* United States v. Conine, 33 F.3d 467, 471 (5th Cir. 1994).

[149] United States v. Leon, 468 U.S. 897, 918 (1984).

[150] *See* United States v. Pace, 898 F.2d 1218, 1231 (7th Cir. 1990).

This can occur when law enforcement seeks a warrant in a different jurisdiction after a previous attempt to secure a warrant is denied. However, during any subsequent trial in the criminal defendant's jurisdiction, the validity of that warrant will be under the scrutiny of the jurisdiction where the defendant is tried, not necessarily where the warrant is issued, thus mitigating in part concerns for magistrate shopping. Unlike the many NIT cases in which the fruits of the search were not suppressed, suppression would be a more appropriate remedy in this situation as a direct violation of Fourth Amendment protections. This would serve as a deterrent for law enforcement agencies which seek a warrant without probable cause or in contravention of the particularity requirement.[151] Additionally, as law enforcement increase its online activities, officers should be held to a higher standard of good faith when seeking warrants which ultimately fail probable cause. Meaning, suppression should be a more appropriate remedy when officers specialize in an area of the law because they are more likely to know if a warrant fails for probable cause despite a magistrate issuing the warrant. However, since suppression is a rare remedy, it is more important for magistrates and applying officers to be increasingly mindful of magistrate shopping.

C. Probable Cause

In future NIT cases, failure to satisfy probable cause to issue a warrant can become a serious problem. This problem would arise in situations not so clear as the FBI's use of NITs for users accessing child pornography websites like Playpen. For websites hosting mixed legal and illegal content, in which illegal content comprises a minor part of the website's content, the use of an NIT should draw more scrutiny. Hacking a computer for accessing the home page of this sort of website should be immediately suspect. Accessing a website in which only a small portion of content is illicit does not create "a fair probability that contraband or evidence of a crime will be found in a particular place." [152] Additionally, if the website hosting illegal content does not have a login page, probable cause should be suspect because there is the increased chance that the user clicked the link to the website by some sort of mistake. To combat these concerns and reduce the risk of violating probable cause requirements of the Fourth Amendment, NITs should only be activated when the accessing computer navigates to pages on the website that contain illicit content.

[151] *Leon*, 468 U.S. at 918.

[152] Illinois v. Gates, 462 U.S. 213, 238 (1983).

D. Fishing Expeditions

Next, changes to Rule 41 may appear to invite fishing expeditions. If the NIT cases are an indication of how these warrants will be used, then fears of fishing expeditions by law enforcement are unfounded. Again, Fourth Amendment restrictions on the scope of search warrants will mitigate undue invasions into citizens' privacy. The Rules do not limit the type of information that can be seized by remote hacking by the government pursuant to a search warrant, so magistrate judges should be wary of issuing warrants which seek to grant the government access to more than simple identifying information of the target computer. Any warrant seeking more than mere identification of the target computer accessing the honeypot creates a much higher risk of violating particularity requirements of the Fourth Amendment. This risk is more acute when a warrant seeks to monitor a computer for an extended period of time.

V. CONCLUSION

The changes to Rule 41(b) and the NIT cases have led to some curious results, but the changes to Rule 41 do not necessarily implicate an expansion of power by the government to infringe upon Fourth Amendment rights. If, during an investigation of online criminal activity, law enforcement restricts its warrant requests to the identifying information of a target computer, then Fourth Amendment rights will unlikely be violated if the target computer triggers the NIT through some reasonably suspect activity online, such as accessing a website where a large portion of the content is illicit, or navigating to a page on the website where there is illicit content.

It will be up to the courts to curb any abuses by law enforcement officers who hack into citizens' computers pursuant to a search warrant. Rule 41 does have broad language which does raise concerns about abuse by law enforcement, but case law is already developing in the NIT cases which will seek to limit the scope of what information may be remotely seized by law enforcement during an investigation of online criminal activity.