# COMMENT

# FIRST THEY CAME FOR THE CHILD PORNOGRAPHERS

**ZOE RUSSELL***



* St. Mary's University School of Law, J.D., 2018. My sincere thanks go to the editing team for their hours of work, Professor John Schmolesky for his mentorship throughout the writing and revision of this Comment, and Federal Public Defender Colin Fieman for providing helpful resources and insightful discussion.

## I. INTRODUCTION

The Department of Justice (DOJ) faces difficulties tackling child pornography websites hosted on services such as The Onion Router (TOR) because these services obscure the identities—namely the Internet Protocol (IP) addresses—of visitors and hosts of suspicious websites.[1] TOR conceals user identities through the employment of a worldwide network of volunteer-operated servers, which direct traffic not in a straight line from user to website, but across a multitude of servers, ultimately masking a user's true IP address behind the IP address of the "exit node" along the chain of volunteer computers.[2]

Law enforcement agents routinely use software to uncover IP addresses of individuals that access or share child pornography on other file-sharing platforms,[3] and courts generally agree an IP address sufficiently identifies a suspect's computer for the purpose of issuing a search warrant at a

1. *See* Mythili Raman, Comment to the Honorable Reena Raggi (Sept. 18, 2013), *in* ADVISORY COMMITTEE ON CRIMINAL RULES, MATERIALS FOR APRIL 7–8, 2014 MEETING, 171–75 (2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [https://perma.cc/CMR9-HVSS].

2. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en [https://perma.cc/QLK8-EK9] ("To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to.").

3. *See* United States v. Thomas, 788 F.3d 345, 347–48 (2d Cir. 2015) ("As part of the investigation, law enforcement relied upon automated software programs to help locate Internet Protocol ('IP') addresses engaged in the possession and distribution of child pornography."), *cert. denied*, 136 S. Ct. 848 (2016); United States v. Brashear, No. 4:11-CR-0062, 2013 WL 6065326, at *1 (M.D. Pa. Nov. 18, 2013) (describing law enforcement use of software program "RoundUp" to scan files across the "Gnutella peer-to-peer file sharing network" for "hash values" related to known child pornography).

physical residence.[4] TOR, however, poses an exceptional challenge to law enforcement by denying capture of IP addresses; even after identifying the server hosting a TOR website, the website's logs do not reveal the true identities of any of its visitors.[5] In response to the challenge of anonymity used to further crimes online, government agencies have increasingly turned to remote access technology beginning at least as early as 1998.[6]

In 2012, the FBI launched its first major operation against child pornography websites using a Network Investigatory Technique (NIT),[7] the FBI's term for their hacking tool.[8] "Operation Torpedo"[9] began with

4. *See* United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007) (attaching a suspect IP address to a physical residence via Internet service provider records furnishes the requisite probable cause to secure a search warrant because a "substantial basis [exists] to conclude that evidence of criminal activity w[ill] be found at [the location]"); *see also* United States v. Chiaradio, 684 F.3d 265, 279 (1st Cir. 2012) ("[T]he magistrate made a sensible determination . . . that a search of the defendant's residence was likely to turn up illicit images."); United States v. Renigar, 613 F.3d 990, 994 (10th Cir. 2010) (noting there was sufficient information to lead "a person of reasonable caution" to conclude that evidence of child pornography "would be found at the residen[ce] . . . in question"); United States v. Vosburgh, 602 F.3d 512, 531 (3d Cir. 2010) (holding the search warrant supported a conclusion that evidence of child pornography would be found at the defendant's apartment).

5. *See* Brad Heath, *FBI Ran Website Sharing Thousands of Child Porn Images*, USA TODAY (Jan. 21, 2016, 12:54 PM), http://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346 [https://perma.cc/8T4X-KR4F] ("When the FBI first realized it could break through Tor," Ron Hosko, former assistant director of the FBI's Criminal Investigative Division, "said the agency gathered counterterrorism investigators and intelligence agencies to see if any of them had a more pressing need for the software").

6. *See* Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2016, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking [https://perma.cc/5H58-3W44] (providing a history of the FBI's publicly known instances of deploying remote access technology).

7. *See* Heath, *supra* note 5 (detailing the 2012 FBI takeover of three child pornography websites resulting in twenty-five indictments).

8. *See* Jonathan J. Wroblewski, Memorandum to the Honorable John F. Keenan (Feb. 7, 2014), *in* ADVISORY COMMITTEE ON CRIMINAL RULES, MATERIALS FOR APRIL 7–8, 2014 MEETING, 245 n.1 (2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [https://perma.cc/7H64-PTV7] (calling attention to the use of the term "hacking" to describe the government's network investigatory technique). The Department of Justice takes umbrage with the term hacking because "[t]he Merriam-Webster Dictionary definition of a hacker is 'a person who illegally gains access to and sometimes tampers with information in a computer system[,]'" whereas the government here seeks lawful authority to gain computer access. Wroblewski, *supra*. In response, Orin Kerr noted the "primary definition provided by the Merriam-Webster Dictionary is 'a person who secretly gets access to a computer system in order to get information, cause damage,'" and the definition selected by Wroblewski "is only the fifth and last alternative definition of the word hacker." Orin Kerr, Memorandum to Members of the Rule 41 Subcomm. (Feb. 8, 2014), *in* ADVISORY COMMITTEE ON CRIMINAL RULES, MATERIALS FOR APRIL 7–8, 2014 MEETING 253 n.1, *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [https://perma.cc/7H64-PTV7]. The Government also bristles at the term malware. *See* United States v.

the arrest of Aaron McGrath, alleged host of three child pornography websites once available through TOR.[10] The FBI sought and received a search warrant to install a NIT onto one of McGrath's websites,[11] which the agency then allowed to operate for three weeks while it monitored activity.[12] The operation "de-anonymized" twenty-five individuals and resulted in nineteen convictions.[13] Unsuspecting users of the website downloaded the NIT alongside their desired file,[14] which communicated to FBI agents the user's "actual IP address" and its "type of operating system[,] . . . version[,] . . . and architecture[.]"[15] Defense attorneys lost their efforts to suppress evidence of the NIT search.[16] However, in legal challenges to the search warrant, defense attorneys did not argue the warrant lacked particularity or violated the jurisdictional requirement of Rule 41(b) of the Federal Rules of Criminal Procedure; rather, they argued the FBI failed to give proper notice to defendants under Rule 41(f)(3).[17]

Although the Federal Government faced little challenge for the NIT's deployment in "Operation Torpedo" cases, United States Magistrate Judge Stephen Wm. Smith issued a surprising ruling in an unrelated case

Jean, 207 F. Supp. 3d 920, 927 n.7 (W.D. Ark. 2016) ("Agent Aflin objects to describing the NIT as malware, because the term has a derogatory connotation . . . . Nevertheless, Agent Aflin concedes that when used as a term of art to explain an ethical hacking technique used by law enforcement, the term malware is descriptive of the NIT used here.").

9. *See* Zetter, *supra* note 6 (describing Operation Torpedo as a "sting operation" which aimed to reveal visitors attempting to mask their identity).

10. *See* Application for a Search Warrant at 19, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015) (revealing McGrath as "Administrator" of the target websites).

11. Search and Seizure Warrant at 3, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015).

12. United States v. Doe, No. 8:13CR107, 2014 WL 5456531, at *1 (D. Neb. Oct. 27, 2014) (describing what is commonly known as a watering-hole attack).

13. Patrick Howell O'Neill, *Former Tor Developer Created Malware for the FBI to Hack Tor Users*, DAILY DOT (Apr. 27, 2016, 9:32 AM), http://www.dailydot.com/layer8/government-contractor-tor-malware [https://perma.cc/RD82-EFBC].

14. *See* NIT Forensic and Reverse Eng'g Report, Continued from Jan. 2015 at 17, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015) ("When an end user accessed a page on a website where the NIT was installed, the NIT code would be se[n]t to the end user[']s computer along with the images/text/content that made up the web page.").

15. Application for a Search Warrant at 32, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015).

16. *See* Memorandum and Order at 10, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015) (compiling and denying fifteen defendants' attempts to suppress evidence seized via NIT in Operation Torpedo).

17. *Id.* at 7–8.

that called into question the FBI and DOJ's strategy for future remote access searches.[18] *In re Warrant to Search a Target Computer at Premises Unknown*[19] pertained to an email user who unlawfully accessed another individual's email inbox in order to invade and transfer money out of that person's bank account;[20] however, the suspect could not be identified because they utilized a proxy server to hide their true IP address.[21] Judge Smith noted the issue to be addressed—whether to approve "a [search] warrant to hack a computer suspected of criminal use"[22]—appeared to be one of first impression in any federal district.[23] He ultimately held, "Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)."[24] Judge Smith denied the warrant, but recognized, "This is

18. *See generally In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (suppressing evidence of a search in which the government deployed remote access technology to identify an individual suspected of federal bank fraud due to the search warrant's lack of particularity and violation of Rule 41(b)).

19. *In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

20. *Id.* at 755.

21. *Id.*

22. *Id.*

23. *See id.* at 756 n.2 (noting although no published opinions exist, a magistrate judge in Washington authorized a similar warrant which aimed to identify the person issuing bomb threats at a high school). Also addressed in the opinion, the Electronic Freedom Foundation submitted a FOIA request to the FBI following the Washington bomb threat, which resulted in a number of documents detailing the regular use of an electronic surveillance tool called "'Computer and Internet Protocol Address Verifier' (CIPAV)." *Id.* at 759 n.10; *see also* Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELECTRONIC FRONTIER FOUND (Apr. 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government [https://perma.cc/GUW9-UWN9] (providing an analysis of the full FOIA return).

24. *In re Warrant to Search*, 958 F. Supp. 2d at 757. The case also turned on lack of particularity because the Government application provided only "indirect and conclusory assurance" that the correct person would ultimately be targeted by the NIT. *Id.* at 759 ("[T]he Government [fails to] explain how it will ensure that only those 'committing the illegal activity will be . . . subject to the technology.'"). The last issue addressed was the Government's failure to meet the requisite burden for video surveillance using a NIT—where the FBI sought to remotely access the subject's computer camera—because the application again offered conclusory statements to show they exhausted alternatives to video surveillance and exerted an effort at minimization. *Id.* at 760. Of note, the FBI requested much greater control over the individual's computer in *In re Warrant to Search a Target Computer* than in "Operation Torpedo" or "Operation Pacifier." *Compare id.* at 755–56 (requesting authority to seize IP addresses, records of Internet activity, logged user names and passwords, documents, email contents, photographs, and control over the computer's built-in camera), *with*

not to say that such a potent investigative technique could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology."[25]

Rule 41(b)(1) of the Federal Rules of Criminal Procedure defines the territorial limitations of a magistrate judge when issuing criminal search warrants:

> 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*[.][26]

Rule 41(b) contains multiple exceptions that confer authority on a magistrate judge to issue search warrants outside of their district, including when property, once located within the district, moves outside of the district after a warrant has issued,[27] investigations of terrorism,[28] installation of a tracking device on property located within the district but that may move outside at some point during the investigation,[29] and to searches of property outside of the fifty states, but inside United States territory, or property of diplomatic and consular missions.[30]

In response to *In re Warrant to Search a Target Computer*, the DOJ began the process of amending Rule 41(b) to provide another exemption for two specific situations faced in the Internet age.[31] The DOJ requested the

Application for a Search Warrant at 40, United States v. Cottom, No. 8:13CR108 8:15CR239, 2015 WL 9308226 (D. Neb. Dec. 22, 2015) (applying for the Operation Torpedo warrant to seize target computers' IP addresses and determine their operating system), *and* Search and Seizure Warrant at 2, United States v. Lorente, No. 2:15-CR-00274 (W.D. Wash. Mar. 7, 2016) (attaching as an exhibit the search warrant affidavit in Operation Pacifier, petitioning the magistrate to authorize the seizure of a site visitor's IP address, operating system, Host Name, operating system username, and media access control (MAC) address).

25. *In re Warrant to Search*, 958 F. Supp. 2d at 761.

26. FED. R. CRIM. P. 41(b)(1) (emphasis added).

27. *Id.* R. 41(b)(2).

28. *Id.* R. 41(b)(3).

29. *Id.* R. 41(b)(4).

30. *Id.* R. 41(b)(5).

31. *See* Mythili Raman, Letter to the Honorable Reena Raggi, *in* ADVISORY COMMITTEE ON CRIMINAL RULES, MATERIALS FOR APRIL 7–8, 2014 MEETING 171–172 (2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [https://perma.cc/7H64-PTV7] (pointing to *In re Search Warrant* as a situation

following addition to Rule 41(b) in a letter to the Advisory Committee on the Criminal Rules on September 18, 2013:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant, to be executed via remote access, for electronic storage media or electronically stored information *located within or outside that district*.[32]

The DOJ illustrated two situations that demanded the change: (1) a situation where the district in which the device is located is concealed through anonymization technology, and (2) to investigate cyber-attacks that infect and seize control over computers in a number of districts, then employ the victimized computers to carry out the attack.[33] Judge Raggi, Chair of the Committee, formed a Subcommittee on Rule 41 to review the suggested change, eventually approving the amendment after minor edits and adding explicit language for the two situations proposed by the DOJ.[34]

---

where underlying facts met Fourth Amendment standards, but not the requirements of Rule 41(b)).

32. *Id.* at 173 (emphasis added). The DOJ also requested a change to the notice provision within Rule 41(f)(1)(C), which was ultimately adopted:

> In a case involving a warrant for remote access to electronic storage media or electronically stored information, the officer executing the warrant must make reasonable efforts to serve a copy of the warrant on an owner or operator of the storage media. Service may be accomplished by any means, including electronic means, reasonably calculated to reach the owner or operator of the storage media. Upon request of the government, the magistrate judge may delay notice as provided in Rule 41(f)(3).

*Id.*

33. *See id.* at 172 (describing the problem of anonymization to further crime as "occurring with greater frequency" and "increasingly common").

34. *See* Sara Beale & Nancy King, Memorandum to Members of the Criminal Rules Advisory Comm., *in* ADVISORY COMMITTEE ON CRIMINAL RULES, MATERIALS FOR APRIL 7–8, 2014 MEETING 161 (2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [https://perma.cc/7H64-PTV7] (forwarding the amendment for publication and public comment in March 2014). The rule's language following publication, public comment, and Supreme Court approval was automatically adopted on December 1, 2016, due to inaction by Congress to oppose the change. *See* Erin Kelly, *Congress Allows Rule Permitting Mass Hacking by Government to Take Effect*, USA TODAY (Nov. 30, 2016, 4:02 PM), http://www.usatoday.com/story/news/politics/elections/2016/11/30/congress-allows-rule-permitting-mass-hacking-government-take-effect/94683030/ [https://perma.cc/5EKU-P94K] (explaining the automatic adoption of the proposed amendment to the rule due to lack of objection by Congress). Federal Rule of Criminal Procedure 41(b)(6) now reads:

> [A] magistrate judge with authority in any district where activities related to a crime may have

While DOJ lawyers pushed for a rule change, FBI agents received a tip about a prolific child pornography website, Playpen, hosted on TOR.[35] They received intelligence from "a foreign law enforcement agency" about the website's true IP address;[36] because the site was mistakenly available on the regular Internet and not only on TOR (with a .onion address), agents were able to identify the site's host as a server in Lenoir, North Carolina.[37] The FBI made a copy of the server. However, due to TOR's relay system, visiting IP addresses were cloaked behind "exit node" IP addresses.[38] Investigators decided to seize and transport the server to an FBI facility in Virginia to run a NIT while tracking visitor downloads.[39] On February 20, 2015, Agent Douglas Macfarlane submitted an affidavit to secure a NIT search warrant with Magistrate Judge Buchanan in the Eastern District of Virginia.[40] Judge Buchanan approved a search warrant to deploy the NIT to search within the Eastern District of Virginia;[41] in addition, Judge Buchannan also authorized a search on those computers "of any user or administrator who logs into the TARGET WEBSITE by entering a username and password."[42] The affidavit described Playpen as a child pornography website hosted on TOR (a hidden service), with special instructions on how to join and add images on the homepage of

> 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: . . . the district where the media or information is located has been concealed through technological means; or . . . in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

FED. R. CRIM. P. 41(b)(6).

35. *See* Joseph Cox, *An Admin's Foolish Errors Helped the FBI Unmask Child Porn Site 'Playpen'*, MOTHERBOARD (May 16, 2016, 11:00 AM), http://motherboard.vice.com/read/an-admins-foolish-errors-helped-the-fbi-unmask-child-porn-site-playpen [https://perma.cc/ZYB3-X7BG] (citing to court documents in which the FBI reveals "a foreign law enforcement agency" tipped them off to Playpen's real IP address, which allowed the FBI to find the physical location of the hosting server).

36. *Id.*

37. *See id.* ("An FBI Agent, acting in an undercover capacity, accessed IP address 192.198.81.106 on the regular internet and resolved to TARGET WEBSITE[.]").

38. *See* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *1 (C.D. Cal. Aug. 8, 2016) ("When a user visits a website located on the Tor network . . . [the] actual IP address is not shown . . . . [Hosts] can only see the IP address of the Tor 'exit node[.]'").

39. *Id.* at *2.

40. Affidavit in Support of Application for Search Warrant at 31, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015).

41. *Id.*

42. *Id.* at 32.

"prepubescent females partially clothed and whose legs are spread[.]"[43] This information lead the affiant—and the magistrate—to conclude that there was probable cause to believe anyone who logged into the site did so with the knowledge and intention to possess or deal in child pornography.[44]

The FBI installed the NIT and re-launched the website from their facility in Virginia, running Playpen from February 20 to March 4 of 2015.[45] Approximately 8,700 computers downloaded a NIT during the Playpen takeover,[46] including computers outside of the United States.[47] After collecting IP addresses on Playpen users, among other identifying information,[48] the FBI conducted physical searches of individual residences for evidence of child pornography and filed charges against a reported 350 defendants.[49]

This Comment will attempt to aggregate the legal challenges taken by the multitude of defendants, many of whom have pooled their efforts into a "national working group,"[50] in Part II. As of this writing, the United States District Court opinions granting their respective defendants'

43. *Id.* at 13.

44. *Id.*

45. United States v. Broy, 209 F. Supp. 3d 1045, 1049 (C.D. Ill. 2016).

46. *See* Transcript of Evidentiary Hearing at 39, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) (detailing discovery received by the defense).

47. *See* United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, slip op. at *3 (D. Minn. Mar. 23, 2017) (noting the revelation that the NIT searched computers in 120 countries during its deployment), *adopted in part and rejected in part*, 2017 WL 3382309 (D. Minn. Aug. 7, 2017); Joseph Cox, *FBI Hacked Computers in Australia as Part of Global Child Porn Sting*, MOTHERBOARD (Oct. 10, 2016, 8:47 AM), http://motherboard.vice.com/read/fbi-hacked-computers-in-australia-as-part-of-global-child-porn-sting [https://perma.cc/XE7L-WAR5] (finding evidence that multiple countries' law enforcement agencies participated in Operation Pacifier, including Australia, Austria, Chile, Greece, and Turkey).

48. Affidavit in Support of Application for Search Warrant at 33, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (approving a collection of the computer's actual IP address, "a unique identifier generated by the NIT," the type of operating system used on the computer, "information about whether the NIT has already been delivered" to the computer, and the computer's Host Name, username, and media access control (MAC) address).

49. *See 'Playpen' Creator Sentenced to 30 Years*, FBI (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years [https://perma.cc/4S5F-CRTP] (breaking down the results of the Playpen investigation in which the FBI claims 350 United States Playpen-based arrests and 548 international arrests).

50. Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, MOTHERBOARD (July 27, 2016, 11:15 AM), https://motherboard.vice.com/read/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen [https://perma.cc/DZ7H-TBS7].

motions to suppress have been reversed under the good faith exception.[51] Multiple other defendants are on appeal from conviction.[52] Part III will address the adoption of the Justice Department's desired language for Rule 41(b) and evaluate the Playpen NIT search warrant affidavit from a Fourth Amendment standpoint of probable cause and particularity.

## II. LEGAL CHALLENGES AGAINST THE PLAYPEN WARRANT AND INVESTIGATION

The sheer number of defendants stemming from the Playpen takeover has led to a growing web of contradictory opinions on a number of legal challenges to the underlying search warrant[53] that observers predict will

51. *See* United States v. Levin, 874 F.3d 316, 318 (1st Cir. 2017) ("We disagree with the district court that suppression is warranted, because the FBI acted in good faith reliance on the NIT warrant."); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017) (reversing the motion to suppress granted by the district court due to the good-faith exception); United States v. Horton, 863 F.3d 1041, 1044–45 (8th Cir. 2017) (overturning two district court decisions granting motions to suppress because the good-faith exception applies).

52. *See* United States v. Chase, No. 5:15-CR-00015-RLV-DCK-1, 2016 WL 4639182 (W.D.N.C. Sept. 6, 2016), *appeal docketed,* No. 17-4675 (4th Cir. Nov. 11, 2017); United States v. Hammond, No. 16-cr-00102-JD-1, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016), *appeal docketed*, No. 17-10340 (9th Cir. Aug. 15, 2017); United States v. Kienast, No. 16-CR-103, 2016 WL 6683481 (E.D. Wis. Nov. 14, 2016), *appeal docketed*, No. 17-1840 (7th Cir. April 21, 2017); United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016), *appeal docketed,* No. 17-4212 (4th Cir. Apr. 11, 2017); United States v. Lough, 221 F. Supp. 3d 770 (N.D. W. Va. 2016), *appeal docketed*, No. 17-4125 (4th Cir. Mar. 2, 2017); *see also* Notice of Appeal, United States v. Taylor, 250 F. Supp. 3d 1215 (N.D. Ala. 2017) (No. 2:16-cr-00203-KOB-JEO-1); Notice of Appeal, United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031 (D. Vermont Apr. 4, 2017); Notice of Appeal, United States v. Gaver, No. 3:16-cr-88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017); Notice of Appeal, United States v. Pawlak, 237 F. Supp. 3d 460 (N.D. Tex. 2017) (No. 3:16-CR-306-D(1)); Notice of Appeal, United States v. Tran, 226 F. Supp. 3d 58 (D. Mass. 2016) (No. 16-10010-PBS); Notice of Appeal, United States v. Owens, No. 16–CR-38-JPS, 2016 WL 7351270 (E.D. Wis. Dec. 19, 2016); Notice of Appeal, United States v. Tippens, No. 3:16-cr-05110-RJB-1, 2016 U.S. Dist. LEXIS 184174 (W.D. Wash. Nov. 30, 2016); Notice of Appeal, United States v. McLamb, 220 F. Supp. 3d 663 (E.D. Va. 2016) (No. 2:16-cr-00092-RBS-RJK); Notice of Appeal, United States v. Jean, 207 F. Supp. 3d 920 (W.D. Ark. 2016) (No. 5:15-CR-50087-001); Notice of Appeal, United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); Notice of Appeal, United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); Notice of Appeal, United States v. Eure, No. 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016); Notice of Appeal, United States v. Werdene, 188 F. Supp. 3d 431 (E.D. Pa. 2016) (No. 15-434).

53. United States v. Broy, 209 F. Supp. 3d 1045, 1048 (C.D. Ill. Sept. 2016) ("[R]easonable jurists can—and have—come to different conclusions on these issues and . . . district judges will await further guidance from the courts of appeals. The Court suggests readers familiarize themselves with previous cases stemming from the warrant at issue in this case before continuing to read this Order.").

wind up in some form in front of the Supreme Court.[54] The challenges against the warrant can be split into two general categories: whether the warrant violated Rule 41(b) of the Federal Rules of Criminal Procedure and whether the search warrant affidavit afforded Magistrate Judge Buchanan enough information to meet the probable cause and particularity requirements of the Fourth Amendment. Part II of this Comment addresses Rule 41(b) and the remedies applied by courts, normally employing the good faith exception to salvage evidence from the exclusionary rule. Part III analyzes probable cause and particularity requirements of the Fourth Amendment, seemingly the only limits on future searches and seizures of this type since Congress enacted the DOJ's desired amendment, Rule 41(b)(6), on December 1, 2016.[55] Reacting to the fact the FBI facilitated the distribution of child pornography through its two-week operation of the site, defendants have also brought motions to dismiss for outrageous government conduct.[56] Lastly, multiple courts heard arguments over whether the FBI must reveal the computer code behind their NIT in discovery, an order the Government has so far refused.[57]

### A. *Whether the Network Investigative Technique Constituted a Search*

In order to violate Rule 41(b)'s jurisdictional requirements for the issuance of a search warrant or the Fourth Amendment protection against unreasonable searches and seizures, the threshold question is whether the

54. *See* Mike Carter, *FBI's Massive Porn Sting Puts Internet Privacy in Crossfire*, SEATTLE TIMES (Aug. 27, 2016, 6:00 AM), http://www.seattletimes.com/seattle-news/crime/fbis-massive-porn-sting-puts-internet-privacy-in-crossfire/ [https://perma.cc/W43C-7QNH] (quoting a senior staff attorney of the Electronic Frontier Foundation); *see also* Stephen Montemayor, *Minnesotans Caught in FBI Child Porn Sting, Raising Constitutional Concerns*, STAR TRIB. (Oct. 9, 2016, 7:58 PM), http://www.startribune.com/minnesotans-caught-in-fbi-child-porn-sting-raising-constitutional-concerns/396472281/ [https://perma.cc/E9RL-U7J8] ("Many legal observers expect the debate to reach the Supreme Court one day.").

55. *See* Kelly, *supra* note 34 (detailing Rule 41(b)(6)'s automatic enactment after a lack of action by Congress to oppose the rule).

56. *See, e.g.*, Carter, *supra* note 52 ("Michaud and other defendants have also sought to have their charges dismissed due to 'outrageous conduct' over the FBI decision to take [Playpen] over and leave the site running.").

57. *See* Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 1–2, United States v. Michaud, No. 3:15-cr-05351RJB (W.D. Wash. May 18, 2016) (outlining the "protracted discovery battle between the parties" in which the court ordered the full NIT code turned over to the defense. The Government appeared willing to comply; yet, ultimately, the Government reversed course and refused disclosure).

hacking tool constitutes a search.[58] To be a search under the Fourth Amendment, the defendant must show the government acquired information by invading a place or thing in which both he and society affords a reasonable expectation of privacy.[59] The conceptual split between the courts depends on how they frame the threshold question: either the defendant enjoys a reasonable expectation of privacy in his computer (a place) or he lacks a reasonable expectation of privacy in his IP address (a thing).[60] The underlying case law determining each question is fairly clear—most courts hold that individuals have a reasonable expectation of privacy in their personal computers;[61] however, most also hold that the third-party doctrine forecloses any expectation of privacy in an IP address.[62] So, while the courts agree the Fourth Amendment does not protect an IP address when retrieved from a third party, the split emerges over whether the third-party doctrine applies where the government retrieves a computer's true IP address through infiltration into the computer rather than pursuant to a subpoena of a third-party in possession of the same records.[63]

58. *See* United States v. Darby, 190 F. Supp. 3d 520, 527–28 (E.D. Va. 2016) (addressing whether the NIT deployment amounted to a search even though the government failed to raise the argument).

59. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *3 (W.D. Tex. Sept. 9, 2016) (recognizing the standards for determining whether a search occurred under the Fourth Amendment (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))).

60. *Compare* United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *4 (M.D. Fla. Aug. 10, 2016) (opposing the conflation of "the expectation of privacy associated with an IP address with the expectation of privacy one has in the computer searched by the NIT"), *with* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *4–5 (C.D. Cal. Aug. 8, 2016) (applying the third-party doctrine to exclude IP addresses from Fourth Amendment protection, and emphasizing an IP address "is not a private physical feature of a computer, but a commonly disclosed digital one assigned by a third party").

61. *See* United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016) ("There appears to be no dispute that [the defendant] Ammons enjoyed a subjective expectation of privacy in the contents of his personal computer." (citing United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013))).

62. *See id.* ("It is true that, as a general proposition, an individual does not possess a reasonable expectation [of privacy] in his IP address." (citing United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016))).

63. *See* United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *18–19 (N.D. Okla. Apr. 25, 2016) ("The Court holds that the property seized was Arterbury's computer. . . . The Macfarlane affidavit makes it clear that the Government could not obtain Arterbury's IP address until its malware made its way back to his computer in Oklahoma and directed it to provide information to the Government."), *adopted by* No. 15-CR-182-JHP, 2016 U.S.

The third-party doctrine was borne out of *United States v. Miller*,[64] in which a defendant argued the subpoena of his bank records violated his Fourth Amendment right against unreasonable searches and seizures of his "private papers."[65] Specifically,

> [R]espondent contends that the combination of the recordkeeping requirements of the [Bank Secrecy] Act and the issuance of a subpoena to obtain those records permits the Government to circumvent the requirements of the Fourth Amendment by allowing it to obtain a depositor's private records without complying with the legal requirements that would be applicable had it proceeded against him directly.[66]

The Court announced "the general rule that the issuance of a subpoena *to a third party* to obtain the records *of that party* does not violate the rights of a defendant[.]"[67] Miller argued the Fourth Amendment should protect his bank records possessed by the bank like it does his personal papers within his home.[68] Yet the Court found Miller lacked a reasonable expectation of privacy in documents he turned over to a third party.[69] The bank records (a thing) could not justify the application of Fourth Amendment protections, but had the records been in his home (a constitutionally protected place), the Fourth Amendment protections would be enforced.[70]

*United States v. Jean*,[71] overturned by the Eighth Circuit on this point,[72] draws similarities between IP addresses in the Playpen cases and telephone numbers in *Smith v. Maryland*,[73] another third-party doctrine case, in which police officers requested a robbery suspect's "telephone company . . .

Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

64. United States v. Miller, 425 U.S. 435 (1976).

65. *Id.* at 440–41.

66. *Id.* at 441 (footnotes omitted).

67. *Id.* at 444 (emphasis added).

68. *See id.* at 441 (arguing the bank subpoenas subvert the Fourth Amendment).

69. *See id.* at 443 (denying a person can maintain a reasonable expectation of privacy in documents turned over to a third party).

70. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals.").

71. United States v. Jean, 207 F. Supp. 3d 920 (W.D. Ark. 2016).

72. United States v. Horton, 863 F.3d 1041, 1046–47 (8th Cir. 2017) (pointing out *Jean*'s flawed analysis because the NIT operates by first searching a place in which society places a reasonable expectation of privacy (citing *Jean*, 207 F. Supp. 3d at 933)).

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

install[] a pen register at [their] central offices to record" all outgoing phone numbers the suspect dialed.[74] The Supreme Court ruled the pen register did not amount to a search because Smith voluntarily turned phone numbers over to the telephone company in order to place calls.[75] However, where the Playpen cases differ—that the search and seizure occurred within the defendants' individual computers rather than within the records of a third party—the Court in *Smith* made sure to emphasize, stating, "Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'"[76]

Multiple courts ruled the defendants in the Playpen cases do not have a reasonable expectation of privacy in their IP addresses, yet offer weak justifications for the intrusion into individual computers to retrieve it.[77] *United States v. Matish*[78] explained "the Government's use of a technique that causes a computer to regurgitate certain information, thereby

74. *Id.* at 737; *see also Jean*, 207 F. Supp. 3d at 933 (deciding the first "hop" to the first TOR node abrogates Jean's subjective reasonable expectation of privacy because his IP address is no longer a "complete secret," and he ought to "assume some measure of risk that TOR's encryption technology could be defeated").

75. *Smith*, 442 U.S. at 743−44.

76. *Id.* at 741. *Florida v. Jardines* recently reinforced protections against physical intrusions of constitutionally protected areas. *See Jardines*, 133 S. Ct. at 1414 ("[T]hough *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[.]'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))).

77. *See* United States v. Dzwonczyk, No. 4:15CR3134, 2016 WL 7428390, at *9 (D. Neb. Oct. 5, 2016) (finding no search of the *computer* occurred because "Defendant's IP address is not a 'physical component' of the computer," but is more akin "to a return address on an envelope"), *adopted by* No. 4:15CR3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016). The court first notes, "absent exigent circumstances, law enforcement could not lawfully conduct a warrantless search of Defendant's home computer to obtain Defendant's IP address." *Id.* at *13. The court, however, inexplicably does not find malware which "compelled Defendant's computer to produce its IP address" to be a search. *See id.* (recognizing there is no need for a search warrant to obtain "an IP address because the IP address itself conveys no substantive information about the user or the contents of the user's online communications"); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *4–5 (C.D. Cal. Aug. 8, 2016) (declaring the defendant had no expectation of privacy in his IP address because he disclosed it to third parties); United States v. Matish, 193 F. Supp. 3d 585, 617 (E.D. Va. 2016) (finding defendant "did not possess a reasonable expectation of privacy in his computer"); United States v. Werdene, 188 F. Supp. 3d 431, 444–45 (E.D. Pa. 2016) ("He was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information.").

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

revealing additional information that the suspect already exposed to a third party . . . does not represent a search" largely because society finds it unreasonable to expect privacy in one's IP address.[79] Taken to its logical conclusion, these courts tacitly approve warrantless encroachment into constitutionally protected spaces as long as law enforcement agents seize only information a defendant at one time shared with a third party;[80] this proposition is clearly foreclosed by the proclamation in *United States v. Jones*[81] that "*Katz* did not erode the principle 'that, when the Government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'"[82]

Another court analogized the use of TOR as an anonymization tool to a case in which a defendant used his neighbor's wireless signal without permission to share child pornography.[83] The defendant accessing the wireless signal did not have an expectation of privacy society would deem "'legitimate' given the unauthorized nature of his transmission."[84] Similarly, the Playpen defendant's "use of T[OR] to view and share child pornography is not only an activity that society rejects, but one that it seeks to sanction."[85] Although people take advantage of TOR worldwide for perfectly legitimate purposes,[86] when "establish[ed] . . . in such an unauthorized manner[,]" the court views the service as one society is not

79. *Id.* at 616–17.

80. *See, e.g.*, United States v. Workman, 205 F. Supp. 3d 1256, 1265 (D. Colo. 2016) ("For example, if Mr. Workman had written his IP address [] down on a piece of paper and placed it on his desk in his home, the government would not be permitted to conduct a warrantless search of his home to obtain that IP address."), *rev'd*, 863 F.3d 1313 (10th Cir. 2017).

81. United States v. Jones, 565 U.S. 400 (2012).

82. *See id.* at 407 (Brennan, J., concurring) (quoting United States v. Knotts, 460 U.S. 276, 286 (1983)) (analyzing whether attaching a GPS device to an individual's vehicle amounts to a search).

83. *See* United States v. Werdene, 188 F. Supp. 3d 431, 445 (E.D. Pa. 2016) (agreeing that an individual does "not have a reasonable expectation of privacy in his wireless internet signal" (citing United States v. Stanley, 753 F.3d 114, 119–22 (3d Cir. 2014))).

84. *See id.* (quoting *Stanley*, 735 F.3d 114 at 120) (recognizing the Third Circuit's decision that an expectation cannot be reasonable when the subjective expectation is not one society is willing to recognize); *see also* Rakas v. Illinois, 439 U.S. 128, 143–44 n.12 (1978) (comparing the defendant to a "burglar plying his trade in a summer cabin during the off season [who] may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate'").

85. *Werdene*, 188 F. Supp. 3d at 445.

86. *See Inception*, TORPROJECT.ORG, https://www.torproject.org/about/torusers.html.en [https://perma.cc/Y3RM-5NPY] (detailing use of TOR by journalists, law enforcement, activists, whistleblowers, business executives, militaries, and IT professionals).

willing to accept.[87]

The Eighth Circuit, along with a majority of district courts, believe the search and seizure took place within a constitutionally protected area because people have a reasonable expectation of privacy in their personal computers.[88] The FBI could not retrieve the IP address without the NIT's invasion of the computer.[89] As *United States v. Darby*[90] illustrates, because FBI agents "plac[ed] code on Defendant's computer, the government literally . . . invaded the contents of the computer."[91]

The most extreme view, laid out in *Matish* but yet to be adopted by any other court, claims a person cannot reasonably expect privacy in their personal computer because, like the broken blinds a police officer peered into in *Minnesota v. Carter*,[92] "Government actors who take advantage of an

87. *Werdene*, 188 F. Supp. 3d at 445–46 (quoting *Stanley*, 753 F.3d at 121).

88. *See* United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017) ("Even if a defendant has no reasonable expectation of privacy in his IP address, he has a reasonable expectation of privacy in the contents of his personal computer."); United States v. Anzalone, 208 F. Supp. 3d 358, 366 (D. Mass. 2016) (finding a NIT deployment searched the defendant's personal computer, which demanded a warrant); United States v. Broy, 209 F. Supp. 3d 1045, 1051–55 (C.D. Ill. 2016) (agreeing with other courts that a NIT requires a warrant); United States v. Ammons, 207 F. Supp. 3d 732, 738–39 (W.D. Ky. 2016) (concluding a NIT constitutes a search for Fourth Amendment purposes and therefore requires a warrant); Report and Recommendation at 11, United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152 (E.D. Tenn. Aug. 26, 2016) ("Although the *information sought*, an IP address, may be information that individuals typically share with third parties . . . the *location to be searched*, the Defendant's computer, is one to which Fourth Amendment protections apply." (citing Riley v. California, 134 S. Ct. 2473, 2492–93 (2014))), *adopted by* Memorandum and Order, No. 3:16-cr-00035-RLJ-CCS (E.D. Tenn. Oct. 11, 2016); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *4 (M.D. Fla. Aug. 10, 2016) ("The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that device is the proper focus of the analysis . . . ."); United States v. Darby, 190 F. Supp. 3d 520, 529–30 (E.D. Va. 2016) (recognizing the Fourth Amendment requires a search warrant if the deployment of the NIT invades the constitutionally protected area of the contents of the individual's computer); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *18–19 (N.D. Okla. Apr. 25, 2016) (concluding the use of malware to obtain and direct the IP address of the defendant back to the FBI constituted a search because the information was not obtainable without seizing the defendant's computer without his knowledge or consent), *adopted by* No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

89. *See* United States v. Workman, 205 F. Supp. 3d 1256, 1264 n.4 (D. Colo. 2016) (rebutting the government's claim that the FBI inevitably could have found the IP address of the defendant; Special Agent Macfarlane, affiant, concluded "the FBI could not obtain Playpen users' IP addresses through other means"), *rev'd*, 863 F.3d 1313 (10th Cir. 2017).

90. United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016).

91. *Id.* at 530.

92. Minnesota v. Carter, 525 U.S. 83 (1998). Concurring in the judgment, Justice Breyer wrote that because a passerby can peer through someone's broken blinds, an officer doing the same should not amount to a search. *Id.* at 104 (Breyer, J., concurring).

easily broken system to peer into a user's computer" are not searching in Fourth Amendment terms.[93] The broken system to which Judge Morgan refers is the now drastically different world of computing from only nine years prior, when the Ninth Circuit decided in *United States v. Heckenkamp,*[94] that an individual retains a subjectively and objectively reasonable expectation of privacy in their network-connected computer.[95] Today, however, as evidenced by multiple examples offered in the opinion,[96] "it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked."[97] The court also emphasized the limited nature of the NIT's scope—only retrieving identifying information—and ruled the NIT does not require a warrant due to the unreasonableness of the expectation of privacy from computer hacking.[98]

### B. *Whether the Magistrate in the Eastern District of Virginia Violated Rule 41(b) by Issuing the Playpen Search Warrant to Remotely Access Computers Outside of the District and, If So, What Is the Appropriate Remedy*

#### 1. Under Which Subsection of Rule 41(b) Does the NIT Warrant Fall?

Defendants largely challenged the Playpen search warrant on the grounds that it violated Rule 41(b) of the Federal Rules of Criminal Procedure.[99] The Federal Magistrates Act, 28 U.S.C. § 636(a), grants United States magistrate judges all "powers and duties conferred or imposed . . . by law or by the [Federal] Rules of Criminal Procedure[.]"[100] Rule 41(b) provides magistrate judges power to issue search and seizure

93. United States v. Matish, 193 F. Supp. 3d 585, 620 (E.D. Va. 2016).

94. United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007).

95. *See Matish*, 193 F. Supp. 3d at 617–18 (citing *Heckenkamp*, 482 F.3d at 1146).

96. *See id.* 619–20 (referring to the government's ability to unlock the Apple iPhone involved in the San Bernardino terrorism case without Apple; the Ashley Madison hack; the Sony Picture breach; multiple exposures of financial data; and the intrusion of a database full of sensitive federal employee personnel records).

97. *Id.* at 619.

98. *Id.* at 620.

99. *See, e.g.*, United States v. Levin, 186 F. Supp. 3d 26, 31 (D. Mass. 2016) (deciding what remedy applies when law enforcement agents execute a search under a warrant issued in violation of Rule 41(b)), *rev'd*, 874 F.3d 316 (1st Cir. 2017). The First Circuit overturned the district court opinion in *Levin* based on the good faith exception without addressing the question of a Rule 41 violation or prejudice standards. United States v. Levin, 874 F.3d 316, 321 (1st Cir. 2017).

100. 28 U.S.C. § 636(a).

warrants, but, unless the investigation falls under a particular exception, restricts the warrant's reach to persons or property located within the magistrate's district.[101] Considering Playpen attracts tens of thousands of visitors,[102] the NIT unsurprisingly searched computers well outside of the Eastern District of Virginia.[103]

The government, in several cases, attempted to differentiate the NIT from a traditional search warrant by applying an exception within Rule 41(b),[104] using both Rule 41(b)(2)—where the property resides within the district at the time of a warrant's issuance, but moves outside of the district before the warrant is executed[105]—and Rule 41(b)(4)—where a tracking device is installed within the district.[106] Several opinions grant the NIT warrant an extraterritorial exception to Rule 41(b), finding it akin to a tracking device, and saving the warrant from violating the rule.[107] Magistrate judges may issue tracking devices from within their districts that

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

102. *See* Transcript of Evidentiary Hearing at 34, United States v. Tippens, No. 16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) (describing discovery from the government which revealed over 100,000 Playpen visitors, approximately 8,700 IP addresses, and 214 resulting arrests throughout Operation Pacifier).

103. *See* Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, MOTHERBOARD (Jan. 22, 2016, 2:01 PM), https://motherboard.vice.com/read/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile [https://perma.cc/FG88-45AD] (cataloging multiple reports of the Playpen warrant's reach into foreign countries); *see also* Transcript of Evidentiary Hearing at 39, United States v. Tippens, No. 16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) (revealing the government uncovered approximately 8,713 IP addresses during Operation Pacifier, of which 7,281 connected back to locations outside of the United States).

104. *See, e.g.*, *Levin*, 186 F. Supp. 3d at 34 (rejecting the use of exceptions under Rule 41(b) as applied to the NIT).

105. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016) (arguing for the use of an exception under Rule 41(b)(2)).

106. *See, e.g.*, United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, slip op. at *6 (D. Neb. Aug. 5, 2016) (analogizing the NIT with a tracking device since the "computer in essence travelled into the district of Nebraska to communicate with the website located in Nebraska" and finding the warrant did not violate Rule 41(b)(4)).

107. *See* Opinion and Order at 15, United States v. Smith, No. 4:15-CR-00467 (S.D. Tex. Sept. 28, 2016) (finding the warrant justified under Rule 41(b)(4)); United States v. Jean, 207 F. Supp. 3d 920, 941–42 (W.D. Ark. 2016) (deciding the warrant was valid according to Rule 41(b)(4)); United States v. Eure, No. 2:16cr43, 2016 WL 4059663, slip op. at *9 (E.D. Va. July 28, 2016) (recognizing that there "were credible arguments that the current rule allowed this warrant"); *Matish*, 193 F. Supp. 3d at 612 (E.D. Va. 2016) (finding the magistrate had authority to issue the warrant despite its potential to exceed the bounds of the magistrates jurisdiction); United States v. Darby, 190 F. Supp. 3d 520, 536–37 (E.D. Va. 2016) ("Rule 41(b)(4) allows a magistrate judge to issue a warrant for a tracking device to be installed in the magistrate's district.").

then travel outside of their districts under Rule 41(b)(4).[108] Although the search of the computer happens outside of the district, courts analogize the NIT to a tracking device because they assume the defendants "digitally touched down in the Eastern District of Virginia when they" visited Playpen during the FBI's hosting.[109] Another court cited to *Kyllo v. United States*[110] for the proposition that government agents in that case used thermal imaging devices to search a home, which the Supreme Court deemed presumptively unreasonable without a warrant.[111] Since the government's intrusion with digital devices constituted a search, analogous to the entering of the home in *Kyllo*, the defendant's entry into Playpen amounted to a digital entry into Virginia.[112] The majority of cases, including the Eighth Circuit's decision in *Horton v. United States*,[113] however, find the warrant falls under the category and territorial requirements of Rule 41(b)(1) and violates the plain meaning of the rule.[114] These cases disagree with the concept that the NIT is similar to a

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

109. *Darby*, 190 F. Supp. 3d at 536.

110. Kyllo v. United States, 533 U.S. 27 (2001).

111. *Matish*, 193 F. Supp. 3d at 612–13 (citing *Kyllo*, 533 U.S. at 40).

112. *Id.* at 613.

113. United States v. Horton, 863 F.3d 1041 (8th Cir. 2017).

114. *See Horton*, 863 F.3d at 1047–48 (rejecting the government's argument of a "virtual" trip resembling a tracking device because the NIT searched computers in Iowa); United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152, slip op. at *2 (E.D. Tenn. Oct. 11, 2016) (finding Rule 41(b)(1) as the applicable subsection for the NIT warrant and ruling the warrant violated the jurisdictional requirements of said rule); *accord* United States v. Allain, 213 F. Supp. 3d 236, 250–51 (D. Mass. 2016) (concluding that the warrant issued by the magistrate for the NIT "technically violated Rule 41(b)"); United States v. Broy, 209 F. Supp. 3d 1045, 1056 (C.D. Ill. 2016) ("Thus, Rule 41(b)(1) did not authorize the magistrate to issue the warrant."); United States v. Croghan, 209 F. Supp. 3d 1080, 1088 (S.D. Iowa 2016) (refusing any comparison between a NIT and a tracking device under an analysis under Rule 41(b)(1)), *rev'd*, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017); United States v. Ammons, 207 F. Supp. 3d 732, 740–41 (W.D. Ky. 2016) (rejecting the Government's interpretation of Rule 41(b)(1)); United States v. Knowles, 207 F. Supp. 3d 585, 599 (D.S.C. 2016) ("The NIT search warrant plainly was impermissible under Rule 41(b)(1) and (2)."); United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *6 (W.D. Tex. Sept. 9, 2016) ("[N]o provision of Rule 41(b) gave the magistrate judge authority to issue the NIT warrant, [therefore] the warrant technically violates Rule 41."); United States v. Workman, 205 F. Supp. 3d 1256, 1261 (D. Colo. 2016) (deciding the NIT warrant was not authorized under the language of Rule 41(b)(1)), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108, slip op. at *3 (N.D. Cal. Sept. 1, 2016) (declaring the NIT warrant was not permissible under Rule 41(b) because the authorized search did not occur in the jurisdiction of the magistrate that authorized the search); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *5 (M.D. Fla. Aug. 10, 2016) (refusing "to expand the authority of the magistrate judge beyond the geographic limitations clearly established by

tracking device in the sense that it does not track, but rather searches and seizes.[115] As such, the warrant must be granted within the district in which the magistrate sits, but "the 'activating computer' [may] never [be] physically present within the [district], and . . . any digital presence of the 'activating computer' [is] insufficient to convey jurisdiction under Rule 41(b)(4)."[116]

2. What Is the Remedy for a Rule 41(b) Violation?

The remedy for a Rule 41 violation varies throughout the circuits, but courts generally follow one of two legal standards.[117] The standard followed by the majority of circuits, described in *United States v. Krueger*,[118] first evaluates whether the violation created a breach of the individual's Fourth Amendment rights.[119] If the rule violation causes a Fourth

Rule 41(b)"); United States v. Werdene, 188 F. Supp. 3d 431, 441–42 (E.D. Pa. 2016) (conceding that Rule 41(b) is applied flexibly, but refusing to extend the Rule to "powers . . . that are clearly not contemplated and do not fit into any of the five subsections" of Rule 41(b) (citing United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, slip op. at *6 (W.D. Wash. Jan. 28, 2016))); United States v. Levin, 186 F. Supp. 3d 26, 33–34 (D. Mass. 2016) (deciding the Government's interpretation of Rule 41(b)(1) fails "because it adds words to the Rule" (citing Lopez-Soto v. Hawayek, 175 F.3d 170, 173 (1st Cir. 1999))), *rev'd*, 874 F.3d 316 (1st Cir. 2017); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *22 (N.D. Okla. Apr. 25) ("[T]his Court finds that the NIT warrant was not authorized by any of the applicable provisions of Rule 41."), *adopted by* No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, slip op. at *5–6 (W.D. Wash. Jan. 28, 2016) (applying Rule 41(b) flexibly still results in a holding that the NIT warrant was invalid).

115. *See Allain*, 213 F. Supp. 3d at 249–50 (setting apart the *Matish* and *Darby* decisions, though finding the tracking device argument plausible); *Henderson*, slip op. at *4 ("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.").

116. *Torres*, slip op. at *5.

117. *Compare* United States v. Krueger, 809 F.3d 1109, 1113−14 (10th Cir. 2015) (differentiating between a violation of constitutional import, which should result in suppression, and a non-constitutional violation, which ought only be suppressed when the defendant can establish prejudice or the intentional disregard of the rule), *with* United States v. Cazares-Olivas, 515 F.3d 726, 730 (7th Cir. 2008) (denying justification of "the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval[,]" due to a violation of federal rules, regardless of any prejudice or deliberateness showing (citing United States v. Trost, 152 F.3d 715, 722 (7th Cir. 1998))).

118. United States v. Krueger, 809 F.3d 1109 (10th Cir. 2015).

119. *See* United States v. Anzalone, 208 F. Supp. 3d 358, 370 (D. Mass. 2016) (citing *Krueger*, 809 F.3d at 1113–14) (finding no Fourth Amendment violation in that the warrant was sufficiently particular and based on probable cause); *Croghan*, 209 F. Supp. 3d at 1089 (following the reasoning of *Krueger* that the court must first determine whether a "violation rises to the level of a Fourth

Amendment violation, the defendant need not make a prejudice showing—although exclusion might still be an inappropriate remedy.[120] If the rule violation does not reach constitutional magnitude, courts should refuse suppression unless the defendant establishes the violation prejudiced her or "there is evidence of intentional and deliberate disregard of a provision in the Rule."[121] The alternative method, followed in the Seventh Circuit, only suppresses evidence found to be lacking in probable cause and without advance judicial approval.[122] The Fifth Circuit follows yet another method, albeit similar to the Seventh, that evaluates the rule violation under a good-faith-exception standard that will be further discussed below.[123]

The only courts to identify the Rule 41 violation as implicating the Fourth Amendment held that a warrant issued by a magistrate without

Amendment violation" (quoting *Krueger*, 809 F.3d at 1113–14)); *Workman*, 205 F. Supp. 3d at 1263 ("The Tenth Circuit's opinion . . . sets forth the analytical framework for determining whether a Rule 41 violation justifies suppression." (citing *Krueger*, 809 F.3d at 1113–14)); Report and Recommendation at 19, United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152 (E.D. Tenn. Aug. 26, 2016) (analyzing whether the defendant suffered a Fourth Amendment violation before moving to the prongs of prejudice or deliberate disregard for the law), *adopted by* Memorandum and Order, No. 3:16-cr-00035-RLJ-CCS (E.D. Tenn. Oct. 11, 2016); *Adams*, slip op. at *7 (agreeing with precedent set in *Krueger* that in "absence of a constitutional violation" Rule 41 demands exclusion only in the presence of "prejudice" or "deliberate disregard of a provision in the Rule" (quoting United States v. Loyd, 721 F.3d 331, 333 (11th Cir. 1983) (per curiam))); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *7 (C.D. Cal. Aug. 8, 2016) (adopting a similar rule to other courts, that exclusion is only available in the presence of a constitutional violation or if the defendant was either prejudiced or can show a deliberate disregard of the rule (citing United States v. Weiland, 420 F.3d 1062, 1071 (9th Cir. 2005))); United States v. Matish, 193 F. Supp. 3d 585, 622 (E.D. Va. 2016) (assessing a Rule 41 violation under the framework of *Krueger* similar to other circuit courts (citing United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000))); *Werdene*, 188 F. Supp. 3d at 442–43 (citing *Levin*, 186 F. Supp. 3d at 34–35) (following a similar standard to *Krueger*, yet differentiating the definition of prejudice used in the Third Circuit).

120. *Krueger*, 809 F.3d at 1113−14.

121. *Id.* at 1114 (quoting United States v. Pennington, 635 F.2d 1387, 1390 (10th Cir. 1980)).

122. *Cazares-Olivas*, 515 F.3d at 730 (citing United States v. Trust, 152 F.3d 715, 722 (7th Cir. 1998)).

123. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *6–7 (W.D. Tex. Sept. 9, 2016) (suppressing evidence only when police are shown to have "engaged in willful, or at the very least negligent, conduct" and, "[a]s such, non-willful violations of Rule 41, where a search is executed pursuant to a warrant, properly supported by an affidavit showing probable cause, and issued by a competent and neutral magistrate judge," suppression should not be an available remedy (first quoting United States v. Leon, 468 U.S. 897, 922 (1984); then citing United States v. Comstock, 805 F.2d 1194, 1210 (5th Cir. 1986)).

jurisdiction renders the warrant void *ab initio*.[124] *United States v. Levin*[125] explains in depth why a violation of subsection Rule 41(b) should be set apart as a substantive provision versus other procedural requirements of Rule 41.[126] The court states:

> Because the violation here involved 'substantive judicial authority' rather than simply 'the procedures for obtaining and issuing warrants,' the Court cannot conclude that it was merely ministerial; in fact, because Rule 41(b) did not grant her authority to issue the NIT warrant, the magistrate judge was without jurisdiction to do so. . . . [B]ecause the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval.[127]

The district court opinion in *Levin* has since been overruled,[128] with the good faith exception nullifying any consideration of Rule 41 as a substantive versus procedural rule. Defendants on appeal in other circuits have attempted to overcome the good faith exception and argue that the rule violation warrants suppression.[129] The district court in *Levin* cites *Krueger* because both cases addressed Rule 41(b),[130] and also happened to involve defendants accused of harboring child pornography.[131]

124. *See Croghan*, 209 F. Supp. 3d at 1090–91 (rejecting the government's argument that defendant's computer was actually searched in the Eastern District of Virginia because his computer accessed the FBI servers in that district; instead, finding the search took place outside of the magistrate's authority, and void *ab initio* (citing *Levin*, 186 F. Supp. 3d at 32–33)); *Workman*, 205 F. Supp. 3d at 1263–64 (agreeing with the *Arterbury* court regarding warrants that are void *ab initio*); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *34 (N.D. Okla. Apr. 25) (concurring with the reasoning of *Krueger* and *Levin*, leading to a decision that the warrant at issue was void *ab initio*), *adopted by* No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016); *Levin*, 186 F. Supp. 3d at 35 (holding "the warrant at issue here was void *ab initio*"). *But see* United States v. Workman, 863 F.3d 1313, 1318–19 n.1 (10th Cir. 2017) ("[T]he warrant here was not void *ab initio*, for the warrant could validly be executed by extracting data from computers within the magistrate judge's district . . . .").

125. United States v. Levin, 186 F. Supp. 3d 26 (D. Mass. 2016), *rev'd*, 874 F.3d 316 (1st Cir. 2017).

126. *Id.* at 35 (quoting United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008)).

127. *Id.* at 36 (citations omitted).

128. United States v. Levin, 874 F.3d 316, 321 (1st Cir. 2017).

129. Brief of the Appellant at 16, United States v. McLamb, No. 17-4299, 220 F. Supp. 3d 663 (E.D. Va. 2016) (attacking the search warrant under Rule 41 as void upon issuance and also on the basis the rule violation prejudiced McLamb).

130. *Levin*, 186 F. Supp. 3d at 36 (citing United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015)) (analyzing the violation of Rule 41(b) under the analytical framework of *Krueger*).

131. *Id.* at 26; *Krueger*, 809 F.3d at 1109.

Investigators in *Krueger* obtained and executed a warrant in the District of Kansas on the defendant's residence; however, the only person at the residence was Krueger's roommate, and Krueger had his cell phone and computer with him.[132] Krueger's roommate informed the Homeland Security Investigations agents about Krueger's whereabouts at another residence in Oklahoma City.[133] An agent then requested and received another warrant from a second magistrate judge in the District of Kansas for a search to be carried out in Oklahoma.[134] The *Krueger* court stopped short of addressing whether the warrant, issued outside of the magistrate's jurisdiction under Rule 41(b)(1), violated Krueger's constitutional rights, or merely infringed on procedural protections, because they found the warrant prejudiced Krueger and required suppression.[135]

Other courts disagree with the district court in *Levin*—that Rule 41(b) is substantive—for a number of reasons. For some, that a person has no reasonable expectation of privacy in their IP address causes the constitutional issue to fall away.[136] Another court found the warrant was not void *ab initio* because "[e]ven if the magistrate judge in the Eastern District of Virginia lacked the authority to issue a warrant that allowed the FBI to deploy the NIT outside of that district, the magistrate judge did have authority to issue a warrant in which the NIT deployed in that district."[137] The Tenth Circuit also adopted this view.[138] Therefore, "[t]he warrant was not void at its issuance."[139] In *United States v. Lough*,[140] the court found the warrant provided everything required by the Fourth

132. *Krueger*, 809 F.3d at 1111.

133. *Id.*

134. *Id.*

135. *Id.* at 1115.

136. *See* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *7 (C.D. Cal. Aug. 8, 2016) ("[N]o violation of 'constitutional magnitude' has occurred here because Defendant had no reasonable expectation of privacy in his IP address." (citing United States v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016))); United States v. Matish, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) ("Generally, one has no reasonable expectation of privacy in an IP address when using the Internet."); *Werdene*, 188 F. Supp. 3d at 443–44 (finding the defendant "had no reasonable expectation of privacy in his IP address").

137. United States v. Anzalone, 208 F. Supp. 3d 358, 372 (D. Mass. 2016); *see also* United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *6 (M.D. Fla. Aug. 10, 2016) (agreeing with other district courts that have concluded that a NIT is not similar to a tracking device, and any issuance of such a warrant by a magistrate judge violates Rule 41(b)).

138. United States v. Workman, 863 F.3d 1313, 1318–19 n.1 (10th Cir. 2017) (citing *Anzalone*, 208 F. Supp. at 372).

139. *Anzalone*, 208 F. Supp. 3d at 372.

140. United States v. Lough, 221 F. Supp. 3d 770 (N.D.W. Va. 2016).

Amendment—sufficient probable cause and particularity in the places to be searched and things to be seized—thus surviving constitutional scrutiny.[141] Similarly, *United States v. Dzwonczyk*[142] lists three requirements of the Fourth Amendment: "(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[;]"[143] and found the warrant met each of these requirements.[144] The district court in *Levin* took issue with the first requirement, finding the magistrate judge had no authority to issue the warrant, which affected "the underlying validity of the warrant."[145]

Utilizing Fourth Amendment standards similar to *Lough*, the court in *Jean* also pointed out that "[a]nother indication that the violation was, if anything, non-fundamental, is the fact that the search warrant could have been authorized by an Article III judge[.]"[146] The Seventh Circuit standard refuses suppression of the evidence unless the violation reaches a constitutional harm,[147] pointing to *United States v. Leon*[148] as foreclosing exclusion based on technical defects in a warrant;[149] whereas those circuits that follow the *Krueger* model continue to evaluate whether a

141. *See id.* at 779 (describing the lengthy FBI affidavit, which provided the magistrate enough to believe evidence of a crime would be found and was limited in the places to be searched "only [to] those users who affirmatively signed into the Playpen site using their screen name and password"); *see also* United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108, slip op. at *4 (N.D. Cal. Sept. 1, 2016) (finding the warrant to comply with the "requirements of probable cause and particularity").

142. United States v. Dzwonczyk, No. 4:15CR3134, 2016 U.S. Dist. LEXIS 141297 (D. Neb. Oct. 5), *adopted by* No. 4:15CR3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016).

143. *Id.* at *21 (quoting United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *7 (M.D. Fla. Aug. 10, 2016)).

144. *See id.* at *21–22 (concluding the warrant in this case met the requirements of probable cause and particularity, however it did not decide neutrality because the issue was not raised by the defendant). The *Dzwonczyk* court also agreed with the Eighth Circuit in *Freeman*, that violations of the rule are only fundamental where the search was "unconstitutional under traditional [F]ourth [A]mendment standards." *Id.* (quoting United States v. Freeman, 897 F.2d 346, 346 (8th Cir. 1990)).

145. United States v. Levin, 186 F. Supp. 3d 26, 35 (D. Mass. 2016) (citing United States v. Glover, 736 F.3d 509, 516 (D.C. Cir. 2013)), *rev'd*, 874 F.3d 316 (1st Cir. 2017).

146. United States v. Jean, 207 F. Supp. 3d 920, 943 (W.D. Ark. 2016).

147. United States v. Hornick, 815 F.2d 1156, 1158 (7th Cir. 1987) (noting "it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the [F]ourth [A]mendment, that would call for suppression").

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

149. *See Hornick*, 815 F.2d at 1158 (holding a Rule 41 violation is technical, not of Fourth Amendment import, and not a conduit to evidence suppression (citing *Leon*, 468 U.S. at 920–21)).

technical violation demands suppression.[150]

Under the *Krueger* framework, if the court finds the violation non-constitutional, or technical, the defendant must show either that he was prejudiced or a provision of the rule was intentionally disregarded in order to qualify for suppression of the evidence.[151] The courts are also split on how the defendant must establish prejudice, with some setting an extremely high bar.[152] Prejudice under *Krueger* is defined "in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed[.]"[153] The prejudice standard in the Ninth Circuit, however, sets a higher barrier—that a search would not have occurred but for the violation.[154] This distinction allows courts to determine ways in which the IP address of the defendant could have been discovered without the particular warrant used, such as explaining "the FBI *could* have installed copies of Playpen in every judicial district in the country (there are 94) and then secured a corresponding number of

150. *See* United States v. Anzalone, 208 F. Supp. 3d 358, 370 (D. Mass. 2016) (agreeing with the analysis of *Krueger* that a Rule 41 violation requires a showing of prejudice or intentional disregard if it does not rise to the level of a constitutional violation); United States v. Workman, 205 F. Supp. 3d 1256, 1263 (D. Colo. 2016) (referencing *Pennington* and *Krueger* as the "analytical framework for determining whether a Rule 41 violation justifies suppression"), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Werdene, 188 F. Supp. 3d 431, 442 (E.D. Va. 2016) (analyzing violations of Rule 41 under the similar framework as *Krueger*, concluding "[t]here are two categories of Rule 41 violations: those involving constitutional violations, and all others" (quoting United States v. Simons, 206 F.3d 392 (403 (4th Cir. 2000))); United States v. Croghan, 209 F. Supp. 3d 1080, 1089 (S.D. Iowa 2016) (adopting the framework of *Krueger* in that "[o]nce a court determines that a Rule 41 violation has occurred, it must next 'determin[e] whether that specific Rule 41 violation rises to the level of Fourth Amendment violation'" (quoting United States v. Krueger, 809 F.3d 1109, 1113–14 (10th Cir. 2015))), *rev'd*, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017).

151. *See Krueger*, 809 F.3d at 1113−14 (quoting United States v. Pennington, 635 F.2d 1387, 1390 (10th Cir. 1980)) (laying out when evidence is suppressible following a violation of a rule governing the execution of a search warrant).

152. *See, e.g.*, *Werdene*, 188 F. Supp. at 446–47 (distinguishing between the Tenth Circuit's prejudice standard and the Third's).

153. *Krueger*, 809 F.3d at 1114.

154. *See* United States v. Welch, 811 F.3d 275, 281 (8th Cir. 2016) (framing the prejudice question as "whether the search would have occurred had the rule been followed" (quoting United States v. Hyten, 5 F.3d 1154, 1157 (8th Cir. 1993))). In this case, the defendant complained the warrant violated Rule 41's notice requirement. *Id.* at 279. The court determined the investigators' failure to notify the defendant of the search within thirty days did not prejudice Welch because "[t]he nature of the investigation indicates they could have easily obtained extensions had they sought them." *Id.* at 281. Therefore, investigators that followed the rule would have obtained the same evidence against the defendant as investigators who did not. *Id.; see also* United States v. Vasser, 648 F.2d 507, 511 (9th Cir. 1980) (asking whether the evidence gathered could have been obtained through other lawful means).

Rule 41 warrants."[155] Another court opined that "[e]ven though difficult for the Government to secure that information tying the IP address to [the defendant], the IP address was public information, like an unlisted telephone number, and eventually could have been discovered."[156] Several more courts point to the fact that a district court judge could have issued the NIT warrant unrestricted by Rule 41, so the defendant cannot show prejudice.[157] The District of Colorado, *United States v. Workman*,[158] found prejudice against the defendant because, had the Rule been followed, the search would not have taken place, and pointing out to the government that the court in *Krueger* asked whether the magistrate judge could have issued the warrant under their own authority.[159] When the government argued the defendant could not be prejudiced due to an unreasonable expectation of privacy in his IP address, the court rejected "[t]he government's prejudice standard [because it] focuse[d] on whether the *evidence* could have been obtained by other lawful means, while *Krueger* ask[ed] whether this particular *search* would have occurred if the Rule had been followed."[160] The Tenth Circuit overturned the district court in *Workman* by assuming, without deciding, that the magistrate judge issued the warrant outside of her authority—which either violated the defendant's constitutional right or prejudiced him—yet finding the good

155. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *7 (C.D. Cal. Aug. 8, 2016).

156. *See* United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, slip op. at *7 (W.D. Wash. Jan. 28, 2016) (describing the Ninth Circuit standard as that found in *Vasser*, where courts are directed to "consider whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, [find] the defendant did not suffer prejudice" (citing United States v. Vasser, 648 F.2d 507, 511 (9th Cir. 1980))).

157. *See* United States v. Jean, 207 F. Supp. 3d 920, 944 (W.D. Ark. 2016) (agreeing with the government's argument that the defendant must show "more than the fact that the defendant would have been better off had the search not been conducted at all"); United States v. Lough, 221 F. Supp. 3d 770, 779–80 (N.D. W. Va. 2016) (ruling no prejudice because a district court judge could legally issue the same warrant (citing *Jean*, 207 F. Supp. 3d at 944)); *cf.* United States v. Workman, 205 F. Supp. 3d 1256, 1263–64 (D. Colo. 2016) (disagreeing with the Government's argument that prejudice does not exist where a district court judge could have issued the same warrant because "the appropriate prejudice inquiry asks whether '*the issuing federal magistrate* judge could have complied with the Rule'" (quoting *Krueger*, 809 F.3d at 1116)), *rev'd*, 863 F.3d 1313 (10th Cir. 2017).

158. United States v. Workman, 205 F. Supp. 3d 1256 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017).

159. *Id.* at 1263–64.

160. *Id.* at 1264.

faith exception applies despite the rule violation.[161]

Finally, the Third Circuit takes an entirely different approach to prejudice by suppressing evidence when the search "offends concepts of fundamental fairness or due process."[162] The court in *United States v. Werdene*[163] explained how investigators could not have found the defendant in any other manner, that they sought out and received the warrant from a neutral and detached magistrate, and that they described in copious detail how the NIT would deploy within their standards of fundamental fairness and due process.[164]

### C. *The Good Faith Exception*

Although a Rule 41 violation may call for suppression of illegally seized evidence, almost all courts ruling on the Playpen warrant, including the First, Eighth, and Tenth Circuits, found the good faith exception of *Leon* and *Herring v. United States*[165] prevented exclusion.[166] Even the courts finding the warrant void *ab initio* split on whether to suppress under the good faith exception.[167] *Leon* announced the good faith exception to the exclusionary rule, whereby courts should not remedy Fourth Amendment violations through suppression of evidence resulting from an illegal search or seizure, if the police officers involved acted in objectively reasonable reliance on a later invalidated search warrant issued by a neutral

161. United States v. Workman, 863 F.3d 1313, 1316–17 (10th Cir. 2017).

162. United States v. Hall, 505 F.2d 961, 964 (3d Cir. 1974).

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

164. *Id.* at 447.

165. Herring v. United States, 555 U.S. 135 (2009).

166. *See* United States v. Levin, 874 F.3d 316, 324 (1st Cir. 2017); United States v. Horton, 863 F.3d 1041, 1052–53 (8th Cir. 2017) (applying the *Leon* exception because any deterrence value of exclusion fails to outweigh the costs); *Workman*, 863 F.3d at 1319 n.3 (distinguishing *Krueger* by pointing out the government waived the good-faith exception in that case); *see also* United States v. Allain, 213 F. Supp. 3d 236, 252 (D. Mass. 2016) (setting apart *Krueger*—in which the court found the good faith exception did not apply where the warrant was void *ab initio*—as an instance in which the officials acted with gross negligence, rather than a more ambiguous question of law with the Playpen NIT).

167. *Compare* United States v. Levin, 186 F. Supp. 3d 26, 40–41 (D. Mass. 2016) (siding with courts deciding that the good-faith exception *does not* apply to warrants which are void *ab initio* (citing United States v. Scott, 260 F.3d 512 (6th Cir. 2001), *overruled by* United States v. Master, 614 F.3d 236 (6th Cir. 2010))), *rev'd*, 874 F.3d 316 (1st Cir. 2017), *with* United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152, slip op. at *1 (E.D. Tenn. Oct. 11, 2016) (refusing to reexamine *Masters* and follow *Scott*, as argued by the defendant, because "[t]his court does not 'reexamine' Sixth Circuit precedent. Instead, this court *follows* it").

magistrate.[168] One court defines objectively reasonable reliance as "whether a reasonably well trained officer would have known that the search was illegal in light of that constellation of circumstances."[169] After *Herring*'s interpretation of *Leon*, the good-faith exception appears nearly impenetrable for defendants attempting to suppress evidence in the face of an invalidated search warrant.[170] The *Herring* interpretation requires a balancing test that analyzes whether "police [mis]conduct [is] sufficiently deliberate that exclusion can meaningfully deter it and sufficiently culpable that such deterrence is worth the price paid by the justice system."[171]

Of those courts that found the NIT prejudiced the defendant, none felt suppression appropriate after accounting for deterrence and the culpability of the police officers.[172] Only courts that found the warrant void *ab initio* resorted to suppression,[173] and of those, the district court decisions in

168. *See* United States v. Leon, 468 U.S. 897, 922–24 (1984) (announcing the good faith exception to the exclusionary rule, which turned the focus of the Fourth Amendment from the occurrence of a violation, to judicially enforced deterrence of reckless or intentional misbehavior by police officers).

169. *Werdene*, 188 F. Supp. 3d at 451 (quoting United States v. Katzin, 769 F.3d 163, 171 (3d Cir. 2014)).

170. *See* United States v. Krueger, 809 F.3d 1109, 1125 (10th Cir. 2015) (Gorsuch, J., concurring) ("Even when an unreasonable search does exist, the Supreme Court has explained, we must be persuaded that 'appreciable deterrence' of police misconduct can be had before choosing suppression as the right remedy for a Fourth Amendment violation." (quoting *Herring*, 555 U.S. at 141)).

171. *Master*, 614 F.3d at 243 (quoting *Herring*, 555 U.S. at 144).

172. *See Scarbrough*, slip op. at *1 (deciding although "the Virginia warrant violates both the Fourth Amendment and Rule 41[,]" *Herring* demands a focus on deterrence of police mistakes, and, here, the magistrate ultimately made the error in judgment); United States v. Allain, 213 F. Supp. 3d 236, 252 (D. Mass. 2016) (finding the NIT amounted to a technical violation, but the good-faith exception applies because FBI agents reasonably relied on the warrant); United States v. Ammons, 207 F. Supp. 3d 732, 744–45 (W.D. Ky. 2016) (applying the good-faith exception even when the warrant is void *ab initio* (citing *Master*, 614 F.3d at 241–43)); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *7 (M.D. Fla. Aug. 10, 2016) (agreeing with the Government's contention that "suppression is a 'last resort,' not the 'first impulse'" (citing *Herring*, 555 U.S. at 140–41)).

173. *See* United States v. Croghan, 209 F. Supp. 3d 1080, 1090–91 (S.D. Iowa 2016) (denying the good faith exception to save the Playpen warrant because it was void *ab initio*), *rev'd*, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017); United States v. Workman, 205 F. Supp. 3d 1256, 1267 (D. Colo. 2016) ("[W]here the warrant is void ab initio under Rule 41(b) the good-faith exception does not apply." (citing United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *34 (N.D. Okla. Apr. 25), *adopted by* No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016))), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); *Arterbury*, 2016 U.S. Dist. LEXIS 67091, at *35 (declaring the good-faith exception inapplicable to a warrant that is void *ab initio* (citing United States v. Levin, 186 F. Supp. 3d 26, 42 (D. Mass. 2016), *rev'd*, 874 F.3d 316 (1st Cir. 2017))); *Levin*, 186 F. Supp. 3d at 42 (holding it was not objectively reasonable for the police officers to rely

*Croghan*, *Workman*, and *Levin* have been overturned by the Eighth and Tenth Circuits.[174]

All decisions finding the warrant void *ab initio* wrangled with Sixth Circuit precedent, the only circuit to have addressed the issue of suppression when a warrant is void at its issuance.[175] *United States v. Scott*,[176] decided in the Sixth Circuit in 2001, refused to apply the good-faith exception to a warrant issued by a judge without authority, because the court did not feel that *Leon* "contemplate[d] a situation where a warrant is issued by a person lacking the requisite legal authority."[177] Nine years later, with *Herring* decided in the interim, the Sixth Circuit reviewed another case where the warrant was issued without appropriate judicial authority;[178] this time the Sixth Circuit found the *per se* rule announced in *Scott* out of step with Supreme Court precedent.[179] Void warrants, versus subsequently invalidated warrants, no longer require suppression under *Master*;[180] rather, courts should apply the *Herring* balancing test to determine whether exclusion is appropriate on a case-by-case basis.[181] While some courts follow *Master* and apply a balancing test focused on police deterrence, others believe *Scott* to be the better decision.[182] The district court in *Levin* applies the exclusionary rule

on the warrant issued by a magistrate judge without jurisdiction to issue the warrant (citing United States v. Glover, 736 F.3d 509, 516 (D.C. Cir. 2013))).

174. *See* United States v. Horton, 863 F.3d 1041, 1052–53 (8th Cir. 2017) (reversing the district court's grant of suppression for the defendants in *Croghan* and *Horton*); United States v. Workman, 863 F.3d 1313, 1321 (10th Cir. 2017) (overturning the district court's decision because the good-faith exception applies).

175. *See, e.g.*, *Levin*, 186 F. Supp. 3d at 39–40 (citing *Master*, 614 F.3d at 236) ("This court is aware of only one federal circuit court to address the question of whether *Leon*'s good-faith exception applies in these circumstances: the Sixth Circuit.").

176. United States v. Scott, 260 F.3d 512 (6th Cir. 2001).

177. *Id.* at 515.

178. *Master*, 614 F.3d at 241.

179. *Id.* at 242.

180. *See* United States v. Lough, 221 F. Supp. 3d 770, 783 (N.D.W. Va. 2016) ("[W]hether the warrant is void *ab initio* or voided at a later date is immaterial to the question presented.").

181. *See id.* at 783 (looking to *Levin*'s analysis of *Scott* and *Master*, but ultimately deciding *Master*'s reasoning fits more in line with Supreme Court doctrine); *Master*, 614 F.3d at 243 ("The Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violations, 'the benefits of deterrence must outweigh the costs.'" (quoting Herring v. United States, 555 U.S. 135, 141 (2009))).

182. *Compare* United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152, slip op. at *1–2 (E.D. Tenn. Oct. 11, 2016) (following *Master* despite arguments by the defendant to the contrary), *with* United States v. Levin, 186 F. Supp. 3d 26, 41 (D. Mass. 2016) (believing an expansion to the good faith exception "improvident" because "courts would have to tolerate

because the void NIT warrant authorized nothing, the NIT performed a warrantless search, and the good-faith exception does not apply to warrantless searches.[183] However, the First Circuit since overturned that decision, looking to *Leon* and ruling out any application of the *Leon* exceptions.[184] The Tenth Circuit overturned the district court in *Workman*, which had adopted *Levin*'s conclusion, because the Supreme Court precedent in *Herring* and *Arizona v. Evans*,[185] applied the good-faith exception even when the agents relied "on warrants that had been recalled or quashed."[186] The mistake here was made by a magistrate judge, so "there was nothing to deter."[187]

In a majority of Playpen cases, courts did not find sufficiently deliberate conduct on the part of the FBI agents in obtaining the warrant for the exclusionary rule to perform its deterrence function.[188] The level of deliberateness should be gross negligence, recklessness, or intentional conduct rather than mere, isolated events of negligence.[189] The balancing act of the good-faith exception also pits the culpability of police behavior against "letting a 'guilty and possibly dangerous defendant[ ] go free'" by suppressing what may be the government's entire case.[190] *Leon* outlined four scenarios in which the balance favors suppression,[191] and which the

evidence obtained when an officer submitted something that reasonably looked like a valid warrant application, to someone who, to the officer, appeared to have authority to approve that warrant application"), *rev'd*, 874 F.3d 316 (1st Cir. 2017).

183. *See Levin*, 186 F. Supp. 3d at 36 (concluding the good-faith exception did not apply to the warrantless search because it was unreasonable for agents to rely on a warrant void *ab initio*).

184. United States v. Levin, 874 F.3d 316, 322 (1st Cir. 2017).

185. Arizona v. Evans, 514 U.S. 1 (1995).

186. *See* United States v. Workman, 863 F.3d 1313, 1319 (10th Cir. 2017) ("How can we say that an agent is unable to rely on a warrant exceeding a magistrate judge's reach if the agent is able to rely on a warrant that doesn't even exist?").

187. *Id.* at 1318–19.

188. *See, e.g.*, United States v. Broy, 209 F. Supp. 3d 1045, 1058 (C.D. Ill. 2016) (lauding the FBI agents involved in obtaining the NIT warrant as "unusually detailed and specific" in their statements to the magistrate rather than condemning their actions).

189. *See* United States v. Ammons, 207 F. Supp. 3d 732, 742–43, 745 (W.D. Ky. 2016) (quoting Davis v. United States, 564 U.S. 229, 238 (2011)) (ruling negligence cannot justify societal costs borne by suppression).

190. *See* United States v. Werdene, 188 F. Supp. 3d 431, 453 (E.D. Pa. 2016) (quoting *Herring*, 555 U.S. at 141) (balancing these costs against the "deterrent effect on law enforcement," and coming to the conclusion that suppressing the evidence "would only serve to 'exact[] a heavy toll on both the judicial system and society at large'" (quoting *Davis*, 564 U.S. at 237)).

191. *See* United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *7 (M.D. Fla. Aug. 10, 2016) (denying the good faith exception in four circumstances: "(1) when 'the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant

Playpen defendants argued applied to the NIT warrant.[192]

Multiple defendants contend law enforcement agents could not reasonably rely on the NIT warrant because it suffered from the glaring facial deficiency of a Rule 41(b) violation.[193] Should nineteen-year veterans of the FBI know Rule 41(b) limited (prior to December 1, 2016)[194] the magistrate judge's authority to issue a warrant outside the district in which she sits?[195] Though some courts believe experienced FBI agents ought to know the limits of Rule 41(b),[196] most point to the varied decisions stemming from the Playpen cases as proof Rule 41(b) is subject to reasonable alternative interpretations.[197] First, they say, courts

knew was false or would have known was false except for his reckless disregard of the truth,' (2) when 'the issuing magistrate wholly abandoned his judicial role,' (3) when the affidavit supporting the application for a warrant is 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable,' and (4) when 'a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid'" (quoting United States v. Leon, 468 U.S. 897, 923 (1984))).

192. *See id.* ("Defendant's argument appears to focus on the fourth category identified by the Supreme Court in *Leon*: facial deficiencies in the search warrant."); *see also* Opinion and Order at 10–11, United States v. Smith, No. 4:15-CR-00467 (S.D. Tex. Sept. 28, 2016) (rejecting defendant's claim that FBI agents acted unreasonably because the agents could not possibly believe all "214,898 members of [Playpen]" resided within Virginia).

193. *See Ammons*, 207 F. Supp. 3d at 743–44 (declining to categorically suppress a void warrant or deny FBI agents the good faith exception when multiple courts questioned Rule 41(b)'s application); *see also* United States v. Dzwonczyk, No. 4:15CR3134, 2016 U.S. Dist. LEXIS 141297, at *26 (D. Neb. Oct. 5) (applying Eighth Circuit precedent, holding even a facially obvious error does not foreclose the good faith exception (citing United States v. Hessman, 368 F.3d 1016, 1021 (8th Cir. 2004))), *adopted by* No. 4:15CR3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016).

194. *See* Kelly, *supra* note 34 (describing opponents' failed efforts to delay enactment of the amended Rule 41(b)(6) on December 1, 2016).

195. *See* United States v. Levin, 186 F. Supp. 3d 26, 42 (D. Mass. 2016) (finding it not objectively reasonable for a nineteen-year veteran of federal law enforcement to be ignorant of the NIT's impropriety), *rev'd*, 874 F.3d 316 (1st Cir. 2017).

196. *See* United States v. Croghan, 209 F. Supp. 3d 1080, 1093 (S.D. Iowa 2016) (determining the agents here sufficiently knowledgeable to doubt the NIT warrant's legality outside of the magistrate's district), *rev'd*, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017).

197. *See* United States v. Horton, 863 F.3d 1041, 1051–52 (8th Cir. 2017) (determining the warrant not facially deficient because multiple district courts ruled it to be facially valid); United States v. Workman, 863 F.3d 1313, 1321 (10th Cir. 2017) (declining to hold law enforcement officers accountable for nuanced legal questions); *Ammons*, 207 F. Supp. 3d at 745 (deciding the different interpretations by several courts, that the warrant was a tracking device under Rule 41(b)(4), was strong evidence the FBI did not act deliberately in violation of the rule by seeking the warrant); Report and Recommendation at 22, United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152 (E.D. Tenn. Aug. 26) (pointing to one-third of the cases related to the Playpen hack concluding the NIT warrant did not violate Rule 41(b)), *adopted by* Memorandum and Order, No. 3:16-cr-00035-RLJ-CCS (E.D. Tenn. Oct. 11, 2016).

should not punish law enforcement officers for not knowing the law when the magistrate made the decision to issue the warrant.[198] The FBI agents sought counsel from DOJ Attorneys, a factor one court explicitly included in the "good faith calculus" to the benefit of the government.[199] Magistrate Judge Franklin Noel, however, in his Report and Recommendation in *United States v. Carlson*,[200] refused to allow the magistrate's judgment to absolve the FBI agents, stating, "the good-faith exception . . . does not stand for the improvident proposition that great deference should be extended to a magistrate judge deliberately or recklessly exercising authority inimical to the source of her statutory power to issue a warrant."[201] Judge Noel also noted the agents' use of 18 U.S.C. § 2705 to extend notice and the request of the use of NIT malware under Rule 41 belies any ignorance of proper procedures.[202] Judge Noels' recommendation, to the extent it granted the defendant's motion to suppress, was not adopted by the district court.[203]

The claim that the Rule 41(b)(6) amendment, instigated by the DOJ, shows knowledge on the part of the DOJ and FBI of jurisdictional limits of the rule can be argued both ways.[204] In *Dzwonczyk*, the addition of Rule 41(b)(6) indicates to the court that Rule 41(b) did not provide authority to Magistrate Judge Buchanan to authorize the Playpen NIT

198. *But see Ammons*, 207 F. Supp. 3d at 745 (distinguishing cases in which law enforcement agents deliberately or recklessly induce the magistrate's mistake).

199. *See* United States v. Katzin, 769 F.3d 163, 181 (3d Cir. 2014) ("We have previously considered reliance on government attorneys in our good faith calculus and concluded that, based upon it in combination with other factors, '[a] reasonable officer would . . . have confidence in [a search's] validity.'" (quoting United States v. Tracey, 597 F.3d 140, 153 (3d Cir. 2010))); *see also* United States v. Werdene, 188 F. Supp. 3d 431, 452 (E.D. Pa. 2016) (explaining reliance on DOJ attorneys provided FBI agents greater confidence in the legality of their actions).

200. United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995 (D. Minn. Mar. 23, 2017), *adopted in part and rejected in part*, 2017 WL 3382309 (D. Minn. Aug. 7, 2017).

201. *Id.* at *10.

202. *Id.* at *9.

203. *See id.* at *1 (relying on the *Horton* decision from the Eighth Circuit, decided on July 24, 2017, which found the good faith exception saved the warrant) (citing United States v. Horton, 863 F.3d 1041 (8th Cir. 2017)).

204. *See, e.g.*, United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *8 (C.D. Cal. Aug. 8, 2016) ("Defendant takes this proposed amendment to mean that the FBI knew it was operating outside Rule 41. But the amendment actually cuts the other way. It would be strange indeed for the Court to suppress . . . in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of warrants like the NIT Warrant.").

warrant.[205] However, in *United States v. Knowles*,[206] the court found it unnecessary to assume the rule change meant evidence found prior to its enactment need be "suppressed as deliberate disregard of the former rule," especially considering the exclusionary rule's purpose is future deterrence.[207] In *Levin*, the First Circuit praised the agents for turning a legal question over to the magistrate for determination, with the caveat that this case is different from one "in which the government would request and somehow obtain a warrant for conduct it knows to be illegal."[208] Other courts refused to fault the FBI agents for the failures of the rule itself, stating, "[T]he instant NIT warrant has brought to light the need for Congressional clarification regarding a magistrate's authority to issue a warrant in the internet age[.]"[209] Second, the exclusionary rule, at least since *Leon*, "operates as a 'judicially created remedy'" to deter police through the suppression of evidence.[210] *Leon* explains the reasoning behind courts excusing Fourth Amendment violations caused by mistakes of judges and magistrates.[211] First, the Supreme Court intended the exclusionary rule to apply to police misconduct rather than judicial errors.[212] "Second, there exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or the lawlessness among these actors requires application of the extreme sanction of exclusion."[213] Lastly, the Supreme Court in *Leon* disbelieved

205. *See* United States v. Dzwonczyk, No. 4:15CR3134, 2016 U.S. Dist. LEXIS 141297, at *7–8 (D. Neb. Oct. 5) (looking to the plain meaning of the rule rather than applying the rule flexibly, as desired by the government), *adopted by* No. 4:15CR3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016).

206. United States v. Knowles, 207 F. Supp. 3d 585 (D.S.C. 2016).

207. *Id.* at 606; *see also* United States v. Tran, No. 16-10010-PBS, 2016 WL 7468005, at *5–6 (D. Mass. Dec. 28, 2016) (regarding testimony by FBI Special Agent Daniel Alfin, that executives at the highest levels of the FBI and DOJ reviewed the Playpen NIT warrant before its submission, as evidence of good faith).

208. United States v. Levin, 874 F.3d 316, 323 n.6 (1st Cir. 2017).

209. United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *7 (W.D. Tex. Sept. 9, 2016); *accord* United States v. Darby, 190 F. Supp. 3d 520, 538 (E.D. Va. 2016) (applauding the FBI for their actions in the face of the rules' inability to keep up with technology).

210. *See* United States v. Leon, 468 U.S. 897, 906–07 (1984) (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)) (introducing the balancing test "resolved by weighing the costs and benefits of preventing the use in the prosecution's case in chief of inherently trustworthy tangible evidence obtained in reliance on a search warrant issued by a detached and neutral magistrate that ultimately is found to be defective").

211. *Id.* at 916–17.

212. *Id.* at 916.

213. *See id.* at 916 n.14 (noting the Court did not find rubber stamp judges to be "a problem of

suppression imposed a significant deterrent effect on judges or magistrates, and the same effect could be had, without the costs of suppression, by an appellate court later ruling the warrant unconstitutional.[214]

Many defendants attempted to get around the barrier of the good-faith exception by claiming the government purposefully misrepresented the NIT's capabilities to the magistrate judge—obscuring the fact the FBI intended the NIT to travel outside the magistrate's district[215]—and by claiming the FBI agents mischaracterized the home page of Playpen at the time the search warrant affidavit was submitted, requesting a *Franks* hearing to introduce outside facts.[216]

In regard to the first claim, the application for the search warrant reads, "I have reason to believe that on the following . . . property *located in the Eastern District of Virginia* there is now concealed" evidence of child pornography offenses.[217] In another section, the affidavit states, "it is respectfully requested that this Court issue a search warrant authorizing . . . the NIT [to] 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 . . . ."[218] The only direct admission within the affidavit that the NIT operates by searching and seizing outside of the magistrate's district is

major proportions").

214. *Id.* at 916 n.15 (1984).

215. *See* United States v. Broy, 209 F. Supp. 3d 1045, 1058 (C.D. Ill. 2016) (arguing "the FBI having two different judges issue warrants is evidence of deliberateness and culpability," which the court dismisses as "rank speculation"); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, slip op. at *8 (M.D. Fla. Aug. 10, 2016) (disagreeing with defendant's contention that no FBI agent with nearly two decades of experience could reasonably rely on the NIT warrant due to Rule 41(b)'s obvious restrictions).

216. *See* United States v. Eure, No. 2:16cr43, 2016 WL 4059663, slip op. at *6 (E.D. Va. July 28, 2016) (denying defendant's request for a *Franks* hearing to show the FBI falsely presented information about the homepage of Playpen—described in the search warrant as an image of two prepubescent girls "in their underwear with their legs spread" apart—versus the homepage's appearance at the time the agents submitted the NIT search warrant affidavit—"a single image beside the site logo of a slightly older child whose legs were crossed and who was wearing stockings and a short dress or top"); *see also* United States v. Allain, 213 F. Supp. 3d 236, 246 (D. Mass. 2016) (finding a *Franks* hearing was not required under these circumstances).

217. Application for a Search Warrant, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (emphasis added).

218. Affidavit in Support of Application for Search Warrant at 29, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (emphasis added).

the term "wherever located," though later the warrant requests authorization to target the computer "of any user or administrator who logs into the TARGET WEBSITE."[219] The disagreement boils down to whether FBI agents presented Magistrate Judge Buchanan enough information to make a decision about authorizing an extraterritorial search warrant.[220] The government argued in one hearing, "[t]he notion that Magistrate Judge Buchanan could have read that . . . [thirty]-page affidavit, and that search warrant[,] and not understood exactly what the government intended to do is preposterous."[221] The defense countered that 7,281 of approximately 8,713 IP addresses discovered through Operation Pacifier—close to 84 percent—originated in foreign countries, yet the warrant affidavit explicitly divulged that the location of the computers may not be within the magistrate's district only once.[222] So far, no district court judges have ruled that the FBI agents acted recklessly or intentionally to mislead Magistrate Judge Buchanan; instead, several believed "FBI agents were, at every juncture, up front with the magistrate judge about how the NIT worked, what it would seize from 'activating computers,' and where 'activating computers' could be located."[223] Magistrate Judge Noel, however, believed agents "recklessly disregarded proper procedure" in requesting the NIT warrant because of the "obvious conflict between the issued warrant, which on its face, was limited to searches in the Eastern District of Virginia, and Agent Macfarlane's affidavit, which sought to search activating computers, wherever on the planet that they were located[,]" specifically faulting Agent Macfarlane for placing the "wherever located" explanation in paragraph forty-six rather than the cover sheet of the warrant application.[224]

219. *Id.* at 32.

220. Transcript of Evidentiary Hearing at 29, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) ("[The government] say[s] that [Judge Buchanan] knowingly signed an unprecedented global warrant for 120 countries . . . that the Department of Justice in its own material says you can't issue . . . .").

221. *Id.* at 45.

222. *Id.* at 39 (producing memos in which the FBI describes Operation Pacifier as an "international investigation").

223. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *8 (C.D. Cal. Aug. 8, 2016); *see also* United States v. Broy, 209 F. Supp. 3d 1045, 1058 (C.D. Ill. 2016) ("[T]he Court finds no indication in this record of any false or misleading statements made to the magistrate in the warrant application that could support an inference of bad faith. On the contrary, the government's efforts in establishing probable cause and obtaining the NIT warrant were unusually detailed and specific.").

224. United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, slip op. at *9

The second claim, involving misrepresentations to a magistrate, involves the appearance of the homepage of Playpen.[225] At some point between authoring the search warrant affidavit and its submission, the homepage changed in appearance from two "prepubescent females partially clothed and whose legs are spread"[226] to "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner."[227] In order to introduce information outside of the four corners of the affidavit, the defense must seek a hearing via *Franks v. Delaware*,[228] first showing the affiant intentionally or recklessly included a false statement in the affidavit, and then that the "statement is necessary to the finding of probable cause."[229] Courts ruled the original homepage image unnecessary for the determination of probable cause due to the amount of other evidence and the suggestive nature of the second image.[230]

The defense in *Jean* argued the FBI's failure "to encrypt the connection between [the defendant's] computer and the FBI server during the deployment of the malware" potentially jeopardized the data's reliability—to the point that FBI agents acted objectively unreasonably to so rely.[231] The court disagreed with the defendant's contention, applying the

(D. Minn. Mar. 23, 2017) (faulting Agent Macfarlane for placing the "wherever located" explanation in paragraph forty-six rather than the cover sheet of the warrant application), *adopted in part and rejected in part*, 2017 WL 3382309 (D. Minn. Aug. 7, 2017). Magistrate Judge Noel also explained his disagreement with other courts' interpretations of the warrant because the additional information on Affidavit A—with a general description of the place to be searched as any activating computer—directly contradicts the geographical limitation on the face of the warrant to the Eastern District of Virginia. *See id.* at *14 ("[T]he Court is aware of no legal authority which stands for the proposition that an affidavit, whether incorporated or not, can expand the scope of a warrant beyond its express limitations; especially an affidavit in direct contradiction to the issued warrant.").

225. *See* United States v. Matish, 193 F. Supp. 3d 585, 606 (E.D. Va. 2016) (finding the defense failed to meet their burden for a *Franks* hearing).

226. Affidavit in Support of Application for Search Warrant at 29, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015).

227. *Matish*, 193 F. Supp. 3d at 595, 606.

228. Franks v. Delaware, 438 U.S. 154 (1978).

229. *Matish*, 193 F. Supp. 3d at 606 (quoting *Franks*, 438 U.S. at 155–56).

230. *See* United States v. Tran, No. 16-10010-PBS, 2016 WL 7468005, at *7 (D. Mass. Dec. 28, 2016) (finding that had Agent Alfin seen the new homepage, but failed to communicate the change such that the affidavit could be updated, his behavior would be reckless; however, since the false statement in the affidavit was not necessary to a finding of probable cause, the court need not address Agent Alfin's actions); United States v. McLamb, 220 F. Supp. 3d 663, 670 (E.D. Va. 2016) (citation omitted) ("The Defendant's statement that the description of the logo on the homepage 'was a pivotal component of the affiant's allegations in support of probable cause,' . . . offends common sense . . . .").

231. United States v. Jean, 207 F. Supp. 3d 920, 938 (W.D. Ark. 2016).

good-faith exception.[232]

The situations outlined in *Leon*, such as facial deficiency of the warrant and misrepresentations to the magistrate, operate within the larger sphere of the rule outlined in *Herring* that in order for the exclusionary rule to apply, the defendant must show "police conduct . . . sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[233]

The courts that found the balance in favor of suppression believed "[e]xclusion of the evidence in this case will serve the remedial and prophylactic purposes of the exclusionary rule" to deter violations of Rule 41(b) of the Rules of Criminal Procedure, "the purpose [of which] is to carry out the mandate of the Fourth Amendment."[234]

Those that weighed against suppression felt the FBI agents acted reasonably rather than culpably.[235] FBI agents generally "did the right thing" by gathering evidence, putting together a detailed affidavit, choosing the federal district most closely related to the target website, and limiting the information seized.[236] As detailed above, most courts found the agents made, at most, negligent mistakes, not sufficiently deliberate for deterrence to "pay its way."[237] On the other side of the balance are "Defendant's general and conclusive argument[s] regarding the need to protect the privacy rights of all citizens . . . ."[238] Or the proposal that "[the defendant] and other viewers and distributors of child pornography can escape capture and continue their viewing and distribution so long as they use Tor, while society and the children victimized by their behavior continue to suffer."[239]

232. *See id.* at 937 (noting reliability of data goes to the weight of the evidence at trial rather than admissibility).

233. Herring v. United States, 555 U.S. 135, 144 (2009).

234. United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *35 (N.D. Okla. Apr. 25), *adopted by* No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

235. *See* United States v. Allain, 213 F. Supp. 3d 236, 251–52 (D. Mass. 2016) (approving the FBI's attempts to comply with rules unable to keep up with technology).

236. United States v. Darby, 190 F. Supp. 3d 520, 538 (E.D. Va. 2016).

237. United States v. Ammons, 207 F. Supp. 3d 732, 743 (W.D. Ky. 2016) (quoting Davis v. United States, 564 U.S. 229, 238 (2011)).

238. United States v. Scarbrough, No. 3:16-cr-00035-RLJ-CCS, 2016 WL 5900152, slip op. at *2 (E.D. Tenn. Oct. 11, 2016).

239. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *8 (C.D. Cal. Aug. 8, 2016).

### D. *Whether the Government Engaged in Outrageous Conduct by Running a Child Pornography Website*

Defendants could seemingly cherry pick language from the exclusionary rule decisions for their arguments of outrageous government conduct because, for a short time, the FBI became "the world's largest distributor of child pornography and re-victimized countless children."[240] Despite facilitating the distribution of over one million images of child pornography to 100,000 visitors of Playpen in order to arrest, so far, 214 people,[241] the claim of outrageous government conduct is almost predestined to fail, and the courts say as much.[242] *United States v. Russell*[243] announced the rule that the government's conduct may be so outrageous "due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction . . . ."[244] No district court, however, felt distribution of child pornography on this scale to be sufficiently shocking to warrant dismissal.[245]

### E. *Discovery Issues Surrounding the Exploit Code of the Network Investigative Technique*

Both the Federal Rules of Criminal Procedure and the Due Process Clause mandate disclosure of evidence material to the guilt or punishment of a defendant.[246] Multiple defendants filed motions to compel discovery of the network investigative technique's source and programming

240. Transcript of Evidentiary Hearing at 36, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016).

241. *See id.* at 34–35 (proposing the ends of Operation Pacifier do not justify the means).

242. *See* United States v. Tran, No. 16-10010-PBS, 2016 WL 7468005, at *3 (D. Mass. Dec. 28, 2016) ("Every district court to consider this same argument has found it wanting."); United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7079617, slip op. at *4 (E.D. Wis. Dec. 5, 2016) (explaining dismissal for outrageous government conduct does not exist in the Seventh Circuit); United States v. Anzalone, 221 F. Supp. 3d 189, 193 (D. Mass. 2016) (finding no dismissals for outrageous government conduct in the First Circuit); United States v. Chase, No. 5:15-CR-00015-RLV-DCK-1, 2016 WL 4639182, slip op. at *1 (W.D.N.C. Sept. 6, 2016) (uncovering not a single case dismissed for outrageous government conduct in the Fourth Circuit or Supreme Court).

243. United States v. Russell, 411 U.S. 423 (1973).

244. *Id.* at 431–32.

245. *See Tran*, 2016 WL 7468005, at *3 (citing other Playpen cases that denied dismissal for outrageous government conduct).

246. *See* United States v. McLamb, 220 F. Supp. 3d 663, 674 (E.D. Va. 2016) (citing FED. R. CRIM. P. 16(a)(1)(E); then citing Brady v. Maryland, 373 U.S. 83, 87 (1963)) (denying defendant's motion to compel discovery because he failed to show materiality).

codes.[247] *Matish* and *United States v. McLamb*[248] denied the motions to compel discovery. In *Matish*, the defendant asserted he needed access to the NIT's exploit code in order to challenge the chain of custody connecting his computer and Playpen, in addition to discovering if the exploit altered his computer security settings, thus exposing him to a third-party attack and possibly planting of evidence.[249] The court felt the defendant rested his claims on speculation and far preferred testimony from FBI Special Agent Alfin, who sat through two cross-examinations and testified he "had no need to learn or study the exploit, as the exploit does not produce any information but rather unlocks the door to the information secured via the NIT."[250] The court believed Agent Alfin's claim that the defendants had nothing to gain from an examination of the exploit code. Balanced against the government's legitimate need to keep secret an important law enforcement tool used to track illegal contraband online, the court easily found the defendant failed to meet his burden of proof.[251]

The defendant in *McLamb* fared similarly to the defendant in *Matish* in his request for the NIT's unique identifier generator and exploit code. The court found his claims—that the code may have defaulted by creating duplicate identifiers, the exploit could have performed outside the warrant's scope, or the exploit could have harmed his security settings—unsupported by any evidence and too speculative to show materiality.[252]

The defense in *Michaud*, on the other hand, won an order compelling discovery of the exploit code.[253] During oral argument, the court agreed with defense counsel's showing of materiality because:

247. *See id.* (requesting the "NIT exploit source code and the unique identifier generator" as material to the defense); United States v. Matish, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016) (acknowledging Defendant's motion to compel discovery of the NIT source or programming code); Motion and Memorandum of Law in Support of Motion to Compel Discovery at 1, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Nov. 11, 2015) (requesting "a copy of the programming code for the 'Network Investigative Technique'" used against the defendant).

248. United States v. McLamb, 220 F. Supp. 3d 663 (E.D. Va. 2016).

249. *Matish*, 193 F. Supp. 3d at 592.

250. *Id.* at 593–94.

251. *See id.* (rejecting defendant's claim regarding chain of custody at the same time).

252. *McLamb*, 220 F. Supp. 3d at 674–75.

253. *See* Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 1, United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. May 18, 2016) (addressing the "government's obligation to disclose the Network Investigative Technique ('N.I.T. code'), a new investigative technology that has presented novel Due Process challenges").

> it comes down to a simple thing. You say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question. And the government should respond under seal and under the protective order, but the government should respond and say here's how we did it.[254]

Despite the order, the government refused to disclose the NIT exploit, and the court responded by excluding evidence resulting from the NIT warrant.[255] The same judge reviewed similar discovery issues in *United States v. Tippens*,[256] where defense counsel pressed at oral argument the need to determine if the NIT operated outside of its permitted scope by seizing unauthorized information.[257] As defense counsel also stressed, the exploit can do more than lock and unlock a computer like Agent Alfin analogized, such as permanently removing security settings and altering data.[258] The judge ultimately ruled against Tippens' discovery motion.[259] Although courts often defer to the knowledge and credibility of federal law enforcement agents, even defenders of the NIT as a law enforcement tool admit the FBI's description of their technology is "deliberately deceptive."[260] The efforts by federal law enforcement to maintain secrecy—both by sealing court documents and battling over discovery—have had and will continue to have lasting negative effects on the justice system.[261]

254. *Id.* at 2–3.

255. Order Denying Dismissal and Excluding Evidence at 1, United States v. Michaud, No. 3:15-CR-05351-RJB-1, 2016 WL 337263 (W.D. Wash. May 25, 2016).

256. United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 30, 2016).

257. *See* Transcript of Evidentiary Hearing at 71, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) (reminding the government the defendant is entitled to discovery for pretrial motions).

258. *Id.* at 71–72.

259. Minute Entry for Proceedings Held Before Judge Robert J. Bryan-CRD, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016).

260. *See* Nicholas Weaver, *Examining an FBI Hacking Warrant*, LAWFARE (Mar. 16, 2016, 8:11 AM), https://www.lawfareblog.com/examining-fbi-hacking-warrant [https://perma.cc/N8CS-MBWV] (pointing to Stingrays—cell site simulators—as another example of deceptive behavior by the FBI, prompting the question: "Is it simply part of the FBI's DNA to attempt to deceive the court?").

261. *See* Consolidated Response to Gov't Motion for Reconsideration; Response to Motions for *Ex Parte* and *In Camera* Procs.; And Second Def. Motion to Dismiss Indictment at 22, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Apr. 25, 2016) (mentioning Stingray cases in which the government opted to dismiss charges rather than reveal their technology).

## III. FOURTH AMENDMENT REQUIREMENTS TO SEARCH WARRANTS BEYOND RULE 41(B)'S SCOPE

Following the enactment of Rule 41(b)(6), warrants of the type used in Operation Pacifier will no longer face procedural hurdles, rather, the substantial provisions of the Fourth Amendment serve as the only bar between residents of the Western District of Texas being hacked into by FBI agents in the Eastern District of Virginia based solely on a magistrate's review.[262] By its sheer scope and operation—uncovering unknown people and locations—the Playpen warrant pushes the bounds of particularity.[263] When not buoyed by a strong showing of probable cause, serving to limit the ability of government agents to act on their own direction, the requirement of particularity ought to increase. While crimes like child pornography offer higher levels of probable cause by the very nature of the crime—it being illegal to view such a pornographic image—other cyber-crimes provide less assurance.[264] With precedent like the Playpen warrant, however, judges may get more comfortable shirking the particularity requirement with weaker showings of probable cause.

262. *Cf.* Transcript of Evidentiary Hearing at 55, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) (responding to government counsel that a Rule 41(b) violation should fall back to the balance of the exclusionary rule, the court replied, "Arguably, to do that you are throwing out Rule 41 and the Magistrate's Act and going right back to the Constitution and saying well, this is a reasonable search, under the Constitution"). *But see* United States v. Krueger, 809 F.3d 1109, 1120 (10th Cir. 2015) (Gorsuch, J., concurring) (seeming to argue that rulemaking bodies do not have the "authority to give magistrate judges any power exercisable anywhere the rulemakers might choose to specify," which "would render Congress's express territorial limitations pointless").

263. The First, Eighth, and Tenth Circuits did not directly address particularity. *See* United States v. Levin, 874 F.3d 316, 322 (1st Cir. 2017) (finding the NIT warrant did not fall under a *Leon* exception in that it was not so "akin to a general warrant and therefore so obviously lacking in particularity that the officers' reliance on it amounted to bad faith" (citing United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents, 307 F.3d 137, 149 (3d Cir. 2002))); United States v. Horton, 863 F.3d 1041, 1049 n.3 (8th Cir. 2017) (declining to address particularity because the court already found a constitutional violation in failure to abide by Rule 41); United States v. Workman, 863 F.3d 1313, 1320 n.4 (10th Cir. 2017) ("Mr. Workman and the amicus curiae also argue that the search was unconstitutional because the warrant lacked particularity. But Mr. Workman and the amicus curiae do not question the executing agents' objective reasonableness in regarding the warrant as adequately particularized.").

264. For example, online markets where illegal contraband is sold, such as the Silk Road, or websites which host propaganda of radical Islamic terrorists. *See* Marcia G. Shein, *Cybercrime and the Fourth Amendment*, THE CHAMPION, July 2016, at 36 (discussing Fourth Amendment issues in the context of cybercrime "ranging from fraud, to internet hacking, to identity theft, to possession, solicitation and distribution of child pornography and beyond").

### A. *The Probable Cause and Particularity Requirements of the Fourth Amendment*

The Fourth Amendment to the Constitution 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 particularly describing the place to be searched, and the persons or things to be seized.[265]

To be reasonable, a search requires a warrant supported by probable cause that a crime occurred, and that evidence of the crime is in a particular location.[266] Law enforcement agents do not face a high bar to show probable cause, the test being whether the affidavit supports a "fair probability that contraband or evidence of a crime will be found in a particular place."[267] Reviewing courts give great deference to the magistrate's rulings, which are reached using common sense reviews of the totality of the circumstances.[268]

Specificity of the warrant turns on particularity and breadth.[269] Particularity means the warrant "suppl[ies] enough information to guide and control the executing agent's judgment in selecting where to search and what to seize . . . ."[270] Overbroad warrants permit law enforcement officers to seize items outside of the proper scope delineated by probable cause.[271] Particularity means "nothing is left to the discretion of the officer executing the warrant."[272]

265. U.S. CONST. amend. IV.

266. *See* United States v. Darby, 190 F. Supp. 3d 520, 531–32 (E.D. Va. 2016) (ruling that common sense suggests the number of steps required to land on the Playpen site, and the appearance of either homepage image, reveal its criminal nature).

267. United States v. Allain, 213 F. Supp. 3d 236, 243 (D. Mass. 2016) (quoting United States v. Rivera, 825 F.3d 59, 63−64 (1st Cir. 2016)).

268. *Id.*

269. *See* United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, slip op. at *4 (W.D. Wash. Jan. 28, 2016) (analyzing whether the NIT warrant lacks specificity to the point of being an unconstitutional general warrant).

270. *Allain*, 213 F. Supp. 3d at 248 (quoting United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013)).

271. *Michaud*, slip op. at *4.

272. Stanford v. Texas, 379 U.S. 476, 485 (1965) (quoting Marron v. United States, 275 U.S. 192, 196 (1927)).

B. *Probable Cause and Particularity Challenges to the Playpen Search Warrant*

In order to show probable cause of a crime, the Playpen website must be so obviously related to the distribution of child pornography that anyone who logged in did so intentionally to view or download child pornography.[273] The magistrate must decide, looking at the totality of circumstances addressed in the affidavit, whether anyone could accidentally land on the Playpen website without knowing, and intentionally entering the site for purposes of viewing child pornography.[274] Defendants attempt to distinguish themselves from other cases involving probable cause based on a paid membership to a child pornography website, arguing Playpen did not require a fee.[275] In addition, the appearance of the homepage plays a major role in deciding whether the average person would assume, in accessing the site, that it is criminal, which resulted in defendants stressing how the homepage image changed between the affidavit's writing and submission.[276] However, the courts each pointed to other factors they found compelling to show probable cause.[277] For example, since Playpen operates on TOR as a hidden service, visitors cannot find the web address through a traditional search engine, but must seek out the address through other online forums.[278] Upon reaching the homepage of Playpen, a message prompted visitors to register, warning visitors not to use a real address or post identifying information.[279] From the foregoing, probable cause

273. *Allain*, 213 F. Supp. 3d at 244.

274. *See* United States v. Darby, 190 F. Supp. 3d 520, 531–32 (E.D. Va. 2016) (arguing it is the duty of the magistrate to decide whether a person could have innocently entered the website and entered information without knowing the content of illegal images contained within).

275. *Allain*, 213 F. Supp. 3d at 244–45.

276. *Id.* at 245.

277. *See* United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, slip op. at *1 (E.D. Wis. Mar. 14, 2016) (calling the steps to reach Playpen "complicated machinations").

278. *See Allain*, 213 F. Supp. 3d at 241 (recognizing disagreements between defense and prosecution on how a defendant may have found Playpen's .onion web address); Epich, slip op. at *1 (finding the steps taken to reach the site made it unlikely that unintentional users would "stumble onto it").

279. *Compare Allain*, 213 F. Supp. 3d at 241 ("Playpen's registration terms, which appeared before users setup a username and password, gave further indication of Playpen's illicit purpose. Prospective registrants were told that, 'the forum operators do NOT want you to enter a real [e-mail] address,' that users 'should not post information [in their profile] that can be used to identify you,' and that, '[t]his website is not able to see your IP.'"), *with* Transcript of Evidentiary Hearing at 33, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016) ("But this warrant, according to them on this probable cause, allowed them to search 100,000 people who just got to the home page, and they conceded that everything else in the home page, the technical language, that

existed to believe searching with a NIT would turn up evidence of child pornography.[280]

Ensuring particularity in a mass computer hack proves more complicated than probable cause. Defendants claim the NIT operates as the "Internet age equivalent of a general warrant."[281] The warrant "gave the FBI too much discretion, applied to too many users, and should have been narrowed to authorize searches of only those site visitors who viewed or downloaded illegal pornography, rather than broadly applying to any visitors that logged into the site."[282] The court in *United States v. Allain*[283] held, however, the number of computers a warrant authorizes to search is irrelevant as long as probable cause exists to search each one.[284] Pointing to the search warrant, the court found limiting the NIT to "any user or administrator who logs into [Playpen] by entering a username and password" appropriately limited the places to be searched to those evidencing probable cause of a crime, and then authorizing the seizure of a few specific pieces of information sufficiently prevented agents from relying on their own discretion.[285]

The magistrate's decision in *United States v. Carlson*[286] offers the only opinion in which the warrant failed for particularity,[287] however the Report and Recommendation was not adopted by the district court.[288] Where other courts defined particularity based on the degree of probable cause to limit agents in their search, and so any computer logging into Playpen provides enough probable cause to be searched, Magistrate Judge Noel finds a timing problem.[289] The place to be searched can only

would not have meant anything to the casual observer, and in fact, it's commonplace for sites like Facebook.").

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

281. *Allain*, 213 F. Supp. 3d at 247.

282. *Id.*

283. United States v. Allain, 213 F. Supp. 3d 236 (D. Mass. 2016).

284. *Id.* at 247.

285. *Id.* at 242; *accord* United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, slip op. at *4–5 (W.D. Wash. Jan. 28, 2016) ("The NIT Warrant does not [] lack sufficient specificity.").

286. United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995 (D. Minn. Mar. 23, 2017), *adopted in part and rejected in part*, 2017 WL 3382309 (D. Minn. Aug. 7, 2017).

287. *Id.* at *11.

288. *Id.* at *8 (rejecting the Report and Recommendation to the extent it grants the defendant's motion to suppress).

289. *Id.* at *11.

be known after the search has already taken place.[290] "As there is no way to identify at the time the search warrant *was issued*, which computers, out of all the computers on planet earth might be used to log into the TARGET WEBSITE, the NIT warrant fails to particularly describe the place to be searched."[291] And although other courts might believe labeling the NIT warrant as "anticipatory" salvages the unknown location of the activating computers, Noel points out that anticipatory warrants must still provide "probable cause to believe that evidence will be found at the particularly described location, if the anticipated event occurs."[292] The failure to identify with particularity the activating computers to be searched meant the warrant only authorized a search within the Eastern District of Virginia, and Carlson's computer in Minnesota was outside of the warrant's scope.[293]

## IV. CONCLUSION

A great divide separates the government's claim of "going dark:"[294] the concern that programs like TOR and strong encryption create a "warrant-proof" space, a space where criminals operate with impunity, and the individual concern of being monitored every waking and sleeping moment by our own devices. A crime like child pornography, universally reviled and recognized for the extreme harm it causes, helps to loosen standards of privacy by influencing balances made in the application of the exclusionary rule, discovery requests, and the analysis of reasonable expectations of privacy. It colors the tools that individuals use for legitimate privacy purposes in order to operate outside of the government's and other interlopers' watchful eyes. The probable cause argument seems strong when analyzing child pornography offenses perpetrated on the web, considering the nature of the websites that deal in peer-to-peer distribution of child pornography. However, *Leon* and its progeny have so watered down the need for probable cause and particularity through the good-faith exception that evidence obtained through other illegal operations involving mass hacking, perhaps facilitated

290. *Id.*

291. *Id.*

292. *Id.* at *13.

293. *Id.* at *13.

294. *Going Dark*, FBI, https://www.fbi.gov/services/operational-technology/going-dark [https://perma.cc/JL7J-AWDA] (describing the phenomenon the FBI seeks to combat with greater surveillance powers).

through a sympathetic magistrate, stand little chance of suppression. For example, TorMail, an anonymous email service operated on TOR, suffered a watering-hole attack, one in which malware automatically downloaded and performed a search of individual computers, based on hitting the home screen.[295] Unsealed court documents show the FBI intended to hack 300 particular email addresses associated with child pornography, but for some reason, installed malware that hacked every TorMail user indiscriminately.[296] The FBI has been less than forthcoming about the botched hack, but if it was an objective mistake, could the evidence be suppressed? Could the NIT go hunting for evidence of a crime against the originally unsuspected TorMail user?

Even in the face of proof that FBI agents, in consult with the DOJ, knew about the facial deficiencies of the Playpen warrant, the good-faith exception operated to salvage seized evidence and its fruit in most cases. Although the Advisory Committee claimed the rule change only affected procedure—that Fourth Amendment safeguards remain in place—the Fourth Amendment, from a remedy standpoint, boils down to a balancing test of society's desire to prosecute criminals, against the ability to deter police misconduct. As one court put it, "Considering the unspeakable harm caused by child pornography, and the creative and limited conduct of the FBI that was undertaken to mitigate that harm, the Court has *no trouble* concluding that suppression is entirely unwarranted here."[297] Despite the Fourth Amendment's very purpose of releasing criminals at the cost of "the sanctity of the person, the home, and property against unrestrained governmental power,"[298] the courts now entertain hyped rhetoric about the costs of letting criminals go free while failing to afford the same deference to constitutional guarantees. Today hacking begins with child pornography, but the newly minted Rule 41(b)(6), which the

295. C. Aliens, *New Documents Reveal the FBI May Have Hacked Every TorMail User Illegally*, DEEPDOTWEB (Nov. 16, 2016), https://www.deepdotweb.com/2016/11/16/new-documents-reveal-fbi-may-hacked-every-tormail-user-illegally/ [https://perma.cc/28XX-KJ3Y] (documenting efforts by the American Civil Liberties Union to unseal court documents after researchers discovered malware installed on a "Down for Maintenance" message displayed on every website hosted by Freedom Hosting, including TorMail).

296. *Id.*

297. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *8 (C.D. Cal. Aug. 8, 2016) (emphasis added).

298. United States v. Leon, 468 U.S. 897, 941 n.8 (1984) (Brennan, J., dissenting) (quoting Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1392–1393 (1983)).

government consistently argued it could interpret flexibly, bears no limitations on types of offenses. Law enforcement officers may request a warrant from any magistrate judge within any district *related to* a crime to search and seize electronic storage media and electronically stored information in any other federal district as long as "the district where the media or information is located has been concealed through technological means."[299] The Playpen opinions so far represent the general acquiescence to law enforcement agencies that act first and account later. As far as motivations and deterrence, the FBI most likely feels incentivized to use their new tool in new and unpredictable ways. The signaling from courts to law enforcement about the Constitution ought to afford a bit more than rhetorical hyperbole in the defense's corner. Decision-making that keeps in mind the exceptional privacy implications of mass hacking demands it. As one judge noted at the end of a hearing, "I have been at this for . . . [forty-eight] years now, and there's some cases that come along that make you feel inadequate, and this is one of them."[300]

299. FED. R. CRIM. P. 41(b)(6)(A).

300. Transcript of Evidentiary Hearing at 73, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (W.D. Wash. Nov. 1, 2016).