Jurisdiction, the Internet, and the Good Faith Exception: Controversy over the Government’s Use of Network Investigative Techniques

Maureen Weidman

Follow this and additional works at: https://ideas.dickinsonlaw.psu.edu/dlr

Part of the Criminal Procedure Commons, Internet Law Commons, Law and Society Commons, Legal History Commons, Legal Writing and Research Commons, National Security Law Commons, and the Privacy Law Commons

Recommended Citation
Maureen Weidman, Jurisdiction, the Internet, and the Good Faith Exception: Controversy over the Government’s Use of Network Investigative Techniques, 122 Dick. L. Rev. 967 (2018).
Available at: https://ideas.dickinsonlaw.psu.edu/dlr/vol122/iss3/10

This Comment is brought to you for free and open access by the Law Reviews at Dickinson Law IDEAS. It has been accepted for inclusion in Dickinson Law Review by an authorized editor of Dickinson Law IDEAS. For more information, please contact lja10@psu.edu.
Jurisdiction, the Internet, and the Good Faith Exception: Controversy over the Government’s Use of Network Investigative Techniques

Maureen Weidman*

ABSTRACT

In February 2015, the FBI discovered a website dedicated to child pornography located on the Tor Network, a network designed to protect its users’ identities on the Internet. Due to the structure of the Tor Network, the FBI could not take down the website and identify users who previously accessed the website. Instead, the FBI kept the website operational for 30 days and applied for a search warrant in the Eastern District of Virginia to use a device called a Network Investigative Technique (“NIT”). This device operated similarly to malware and “attached” to computers accessing the website, allowing the government to identify individuals who accessed the website from districts throughout the country.

The NIT proved successful in identifying numerous offenders throughout the United States, many of whom are now challenging the validity of the NIT warrant. Many of these defendants claim that the magistrate judge in the Eastern District of Virginia lacked jurisdictional authority to issue the warrant under Federal Rule of Criminal Procedure 41(b). This very rule was amended in December, 2016 to explicitly allow magistrate judges to issue warrants outside their districts in cases where defendants have concealed their locations through technological means.

This Comment discusses how district courts have handled motions to suppress evidence from the NIT warrant. Most courts have found that the NIT warrant violated Rule 41(b) but have applied the good faith exception to the warrant requirement and denied suppression of evidence seized as a result of the NIT war-

* J.D. Candidate, The Dickinson School of Law the Pennsylvania State University, 2018.
rant. This Comment addresses the amended Rule 41(b)’s possible retroactivity, as well as how courts should view the validity of the NIT warrant if the amendment is not retroactive. Lastly, this Comment analyzes the applicability of the good faith exception in light of the new amendment, the failure of the good faith exception to regulate magistrate judges who overstep jurisdictional boundaries, and possible solutions to regulate magistrate judges’ conduct.

**Table of Contents**

I. **Introduction** .......................................................... 968

II. **Background** ......................................................... 971
    
    A. The Playpen Website and the Tor Network ............. 971
    B. Rule 41(b) of the Federal Rules of Criminal Procedure and its New Subsection ... 975
        1. Rule 41(b) as it Appeared in February 2015 ... 975
        2. The New Subsection of Rule 41(b) ............. 977
    C. The Good Faith Exception ................................. 978
    D. Cases Rejecting the NIT Warrant ..................... 978
    E. Cases Upholding the NIT Warrant .................... 980
    F. The Possibility of Retroactivity .................... 983

III. **Analysis** .......................................................... 985
    
    A. The Changes to Rule 41(b) Most Likely Do Not Apply Retroactively ......................... 985
    B. Denying Suppression Is Consistent with the Spirit but Not the Letter of Rule 41(b) ...... 986
    C. Policy Arguments in Favor of Denying Suppression ................................................... 988
    D. Possible Ways to Ensure Magistrate Judges Do Not Overstep Jurisdictional Boundaries ... 990
    E. The New Subsection and the Good Faith Exception .................................................... 992

IV. **Conclusion** ......................................................... 994

I. **Introduction**

As crime continues to occur more frequently on the Internet, the government has sought new and creative ways to detect certain criminal activity. The government has employed the use of certain methods...

---


devices known as “Trojan” devices, which purport to be harmless to the users in order to invade computers and extract information. A number of different types of Trojan devices exist, such as data extraction software, Network Investigative Technique (“NIT”), remote search, and Computer and Internet Protocol Address Verifier (“CIPAV”).

Trojan devices, specifically the NIT, provide a great benefit to government investigators, as criminals frequently use anonymizing software to avoid detection. Criminals are known to frequent certain areas of the Internet, such as the Tor Network. The Tor Network’s structure makes tracking users through traditional means virtually impossible, a subject that this Comment will discuss in greater detail.

Despite their utility in detecting otherwise hidden criminal activity, NITs and other Trojan devices are controversial. As one scholar notes in her article on Foreign Intelligence Surveillance Act (FISA) Reform, “the privacy interests involved in NIT are substantial.” In other contexts, courts have noted the degree of information stored on computers and cell phones, and therefore the need to protect these devices. In light of the volume of information stored on electronic devices, the use of Trojan devices such as NITs is alarming.

Aside from the social concerns, a number of legal issues arise with the use of NITs, not the least of which involve jurisdiction over

4. Id.
5. Id.
8. See infra Part II.A.
10. Id.
11. See United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (“Electronic devices are capable of storing warehouses full of information. . . . Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.”).
12. See Donohue, supra note 9, at 623.
Internet users. In the Internet age, the traditional notion of jurisdiction based on geographical boundaries is far more difficult to maintain. NITs and other Trojan devices function remotely, reaching out and attaching to computers outside the district where the devices are located. As one scholar points out, the FBI has argued that the use of Trojan devices does not require jurisdictional authorization. However, this assertion appears to fly in the face of the Federal Rules of Criminal Procedure, which outline and provide restrictions for jurisdictional authority of magistrate judges. No doubt, the use of Trojan devices presents the courts with unique jurisdictional issues it must address.

In February of 2015, courts were presented with an interesting case involving a magistrate judge in the Eastern District of Virginia who issued a search warrant allowing a search that extended outside her district through the Internet. If NIT warrants require jurisdictional authority, the next question is whether magistrate judges can issue warrants outside of their districts. Courts do not

13. See United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017) (discussing the jurisdictional limitations implied in Rule 41(b) affecting the validity of the NIT warrant); United States v. Werdene, 188 F. Supp. 3d 431, 452 (E.D. Pa. 2016) (discussing the magistrate judge’s mistaken belief that she had jurisdiction to issue the NIT warrant).


15. See Hennessey & Weaver, supra note 7.


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

18. See Donohue, supra note 9, at 623–24 (discussing the different views on what level of protection to give electronic devices in light of new methods of government surveillance).


20. Owsley, supra note 3, at 320 (discussing the various ways in which magistrate judges can have authority to issue a warrant within and outside of their jurisdictions).
agree on this issue. Courts also do not agree on whether the government should nevertheless be able to use the fruits of the search based on the good faith exception to the exclusionary rule. This Comment seeks to address a number of issues, including the jurisdictional questions raised by the use of NITs. Some articles address the government’s use of NITs in a general sense. This Comment will focus on a recent set of cases arising from a warrant in the Eastern District of Virginia and the effect of the recent amendment to Fed. R. Crim. P. 41(b). Also, this Comment will address how the amendment could change the application of the good faith exception to these cases. Finally, this Comment will discuss the exclusionary rule, the rule’s failure to regulate magistrate judges, and possible solutions to the issue of regulating magistrate judges’ conduct.

II. BACKGROUND

A. The Playpen Website and the Tor Network

In December of 2014, the FBI received information from a foreign law enforcement agency regarding a website dedicated to child pornography called “Playpen.” In order to access the majority of the website’s content, visitors to the website logged in with a username and password. In total, the Playpen website had over 150,000 users who created usernames and passwords to access the website. Playpen contained tens of thousands of pornographic images of children, which were “highly categorized” based on the ages of the children as well as the types of activities depicted. The website also contained forums that allowed the users of the website

21. See Eure, 2016 WL 4059663, at *8 (holding that the warrant did not violate Rule 41(b)); see also United States v. Levin, 186 F. Supp. 3d 26, 34 (D. Mass. 2016), vacated, 874 F.3d 316 (1st Cir. 2017) (holding that the magistrate judge lacked jurisdictional authority to issue the warrant under Rule 41(b)).
22. See Anzalone, 208 F. Supp. 3d at 372 (applying the good faith exception); see also Levin, 186 F. Supp. 3d at 41–42.
23. See generally Owsley, supra note 3 (discussing Trojan devices and whether they are authorized by Federal Rule of Criminal Procedure 41(b)).
25. See infra Part III.E.
26. See infra Part II.C.
27. See infra Part III.E.
31. Id.
to communicate ideas with one another about grooming victims and avoiding detection. Based on the information provided by the foreign law enforcement agency and information from its own investigation, the FBI determined the location of the website’s operator and searched his Florida home on February 19, 2015. The FBI then took control of the website’s server on February 20, 2015.

After taking control of the website, the government applied for a search warrant in the Eastern District of Virginia to keep the website operational. Normally, the government would be able to “take down” the website and retrieve information regarding the website’s visitors, but due to the website’s location on the Tor Network, this was not possible. The Tor Network disguises its users’ identification information by sending the information through relay computers. On the Tor Network, the Internet protocol, or “IP” address, that would appear in an IP log is that of the last computer in this chain of relay computers, not the computer that accessed the website. Therefore, IP addresses cannot be traced on the Tor Network.

Users can access the Tor network by downloading a Tor browser. Some Internet content, such as “hidden services,” appears only on the Tor network, and users cannot find these websites

32. Grooming is a type of behavior often exhibited by sex-offenders which involves developing a close relationship with a child and giving the child gifts and special attention prior to molesting the child. See Marjorie A. Shields, Annotation, Admissibility of Expert Testimony on Grooming Behavior Involving Sexual Conduct with Child, 13 A.L.R. 7th Art. 9 (2016).
34. Id.
35. Id.
36. Id.
37. The agent that applied for the search warrant explained the difficulties the FBI encountered in overcoming the masking capabilities of the network specifically saying that “other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried.” United States v. Werdene, 188 F. Supp. 3d 431, 438 (E.D. Pa. 2016) (quoting the FBI’s application for a search warrant).
38. The word “Tor” is an acronym for “The Onion Router.” For more information about the Tor network, see Tor: Hidden Service Protocol, Tor Project: Anonymity Online, https://www.torproject.org/docs/hidden-services.html.en. (last visited Jan. 9, 2017).
41. An IP address is a unique code that identifies a computer or other device. See Understanding TCP/IP Addressing and Subnetting Basics, Microsoft, https://support.microsoft.com/en-us/kb/164015 (last visited Dec. 8, 2017).
42. Anzalone, 208 F. Supp. 3d 358 at 361.
43. Matish, 193 F. Supp. 3d at 593.
using ordinary search engines. The Tor Network, originally created by the U.S. Naval Research Laboratory to protect government communications, is now reputed to be a haven for criminal activity.

Due to the challenges created by the Tor network in detecting criminals, the government used a different strategy than it would normally use in order to ascertain the IP addresses of those individuals accessing the website. Even if the government successfully located the IP logs for the Playpen website, the IP addresses on the logs would reflect only the IP addresses of the last computers in the “chain” of relay computers. The logs would not contain the IP addresses of those accessing the website. While the government could have “taken down” the website as it would normally do, the anonymity of the Tor Network made it impossible for the government to obtain the information it needed: the users’ IP addresses.

Due to the difficulties in obtaining criminals’ IP addresses, the government chose to keep the website operational from February 20 to March 4, 2015. The government applied for a search warrant in the Eastern District of Virginia to use a device called a NIT. The NIT functions similarly to malware, attaching to computers. Signals from one computer to another are sent through a circuit of these volunteer-operated servers or “relay” computers. This makes it difficult, if not impossible, for these signals to be traced. For more details, see Tor Project: Anonymity Online, supra note 38.

44. The Tor network functions using volunteer-operated servers. Signals from one computer to another are sent through a circuit of these volunteer-operated servers or “relay” computers. This makes it difficult, if not impossible, for these signals to be traced. For more details, see Tor Project: Anonymity Online, supra note 38.

45. Matish, 193 F. Supp. 3d at 593.

46. See Tor Project: Anonymity Online, supra note 38.

47. Researchers at King’s College in London found that 57 percent of websites on the Tor network are used for criminal activity. See McGoogan, supra note 1. Regarding child pornography specifically, in 2011, the “hacktivist” group Anonymous took down the website Lolita City, which was a child pornography website located on the Tor Network. Sean Gallagher, Anonymous Takes Down Darknet Child Porn Site on Tor Network, ARS TECHNICA (Oct. 23, 2011, 7:00 PM), http://arstechnica.com/business/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network. The takedown was part of Anonymous’s anti-child-pornography effort called “Operation Darknet.” Id.

48. See Matish, 193 F. Supp. 3d at 594.


50. Id.

51. See Matish, 193 F. Supp. 3d at 594.

52. Id. (“The FBI did not immediately shut Playpen down; instead, it assumed control of Playpen, continuing to operate it from a governmental facility in the Eastern District of Virginia from February 20, 2015 through March 4, 2015.”).


54. “Malware” refers to “malicious software” or software programs designed to do harm to computers. Per Christensson, Malware Definition, TECHTERMS, https://techterms.com/definition/malware (last visited Dec. 28, 2017). The court in Matish declined to consider whether the NIT actually is a form of malware, but
puters that access the website.\textsuperscript{55} The NIT did this by augmenting content from the Playpen website with instructions that caused the activating computers to transmit information like IP addresses.\textsuperscript{56} The NIT would deploy when users logged in with a username and password.\textsuperscript{57} The NIT is made up of four parts, one of which is called the “exploit.”\textsuperscript{58} The exploit has been compared to a person opening a window to a house that the homeowner believed was locked.\textsuperscript{59} The exploit allows other parts of the NIT to “enter” the computer and extract data.\textsuperscript{60} Exactly how the exploit functions, though, remains undisclosed by the government.\textsuperscript{61}

The government used the information it gathered from the exploit in an affidavit prepared by a special agent.\textsuperscript{62} The affidavit in support of the search warrant indicated that the NIT would cause “activating computers” to reveal their subscriber information wherever the computers were located.\textsuperscript{63} Therefore, the warrant authorized the government to search computers located outside of the Eastern District of Virginia.\textsuperscript{64} The magistrate judge approved the search warrant, and law enforcement deployed the NIT as planned.\textsuperscript{65}

After collecting IP addresses through the NIT, the government subpoenaed Internet service providers to obtain the names and locations associated with the IP addresses.\textsuperscript{66} Ultimately, the NIT led to the prosecution of 137 criminal cases.\textsuperscript{67} Defendants from a variety of districts have challenged this initial search warrant in the Eastern District of Virginia in an attempt to exclude evidence from subsequent searches.\textsuperscript{68} Due to the exclusionary rule, an attack on

\textsuperscript{55} See Nakashima, supra note 2.
\textsuperscript{56} Anzalone, 208 F. Supp. 3d at 364.
\textsuperscript{58} Hennessey & Weaver, supra note 7.
\textsuperscript{59} Id.
\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{63} Id. at 364.
\textsuperscript{65} Id.
\textsuperscript{66} Id.
\textsuperscript{67} Hennessey & Weaver, supra note 7.
this initial search warrant would leave the government with no evidence to further its case.69

One of the most popular challenges to the search warrant, which has been accepted by various courts, targets the magistrate judge’s lack of jurisdiction over defendants outside the Eastern District of Virginia.70 The Federal Rules of Criminal Procedure, particularly Rule 41(b), govern magistrate judges’ jurisdiction for issuing warrants.

B. Rule 41(b) of the Federal Rules of Criminal Procedure and its New Subsection

Rule 41(b) of the Federal Rules of Criminal Procedure sets forth a magistrate judge’s authority to issue a warrant.71 The Rule currently contains six subsections, the sixth having gone into effect on December 1, 2016.72

1. Rule 41(b) as it Appeared in February 2015

The first subsection reads, “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.”73 This subsection establishes the general principle that magistrate judges have authority to issue warrants within their districts. However, magistrate judges are not necessarily confined by the bounds of their jurisdictions, which the remaining subsections of Rule 41(b) demonstrate.74

Under Rule 41(b)(2), a magistrate judge can issue a warrant for a “person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is

585 (E.D. Va. 2016) (considering defendant’s motion to suppress evidence seized from his home computer); Michaud, 2016 WL 337263.

69. See Wong Sun v. United States, 371 U.S. 471, 488 (1963) (holding that evidence discovered by law enforcement through exploitation of an illegal search may not be used against a defendant); see also Werdene, 188 F. Supp. 3d at 453 (acknowledging that the government would have no case without the evidence from the NIT warrant).


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

72. Id.

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

74. FED. R. CRIM. P. 41(b).
executed.” This subsection could potentially apply to cases dealing with the Internet, but much of the case law surrounding Rule 41(b)(2) does not apply to Internet searches.

Under Rule 41(b)(4), a magistrate judge may issue a warrant “to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.” This exception to the general rule of Rule 41(b) applies in cases like *United States v. Jones*,79 where the police attached a tracking device to the underside of a car. However, courts often cite to 41(b)(4) when confronted with NIT-related warrants.81 Congress’s intent when drafting 41(b)(4) may have been to allow an exception to the general rule in 41(b) for situations like the one in *Jones*, but 41(b)(4) could be interpreted more broadly to include cases dealing with Internet jurisdiction.82 This Comment will address the arguments presented by courts that have applied Section 41(b)(4) to the NIT warrant used in the Playpen case.

Under 41(b)(5), a magistrate judge “having authority in any district where activities related to the crime may have occurred . . . may issue a warrant for property that is located outside the jurisdiction of any state or district.”84 For instance, a magistrate judge may issue a warrant for property located in any U.S. territory, premises owned by the United States, or residence or appurtenant land

75. FED. R. CRIM. P. 41(b)(2).
78. FED. R. CRIM. P. 41(b)(4).
80. Id. at 403.
82. See United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016) (finding that the NIT is analogous to a tracking device).
83. See infra Parts III.D–E.
84. FED. R. CRIM. P. 41(b)(5) (emphasis added).
leased by the United States. The broad language of this subsection, referring to “any district where activities related to the crime may have occurred,” may allow a magistrate judge in a district where a computer server is located to issue a warrant outside the district but within a U.S. territory. For website searches, the question posed by 41(b)(5) is whether the activity “occurred” in the district that contains the computer server. This subsection eliminates the need for the object of the search to be located in the district, but would not apply if activities related to the crime did not occur in the magistrate judge’s district.

2. The New Subsection of Rule 41(b)

Lastly, 41(b)(6) adds another situation where a magistrate judge can issue a warrant outside his or her district. The language of the new subsection reads:

A magistrate in authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The language of the new subsection appears to authorize magistrate judges to issue warrants like the NIT warrant in the Playpen case. The subsection’s reference to “remote access” would apply to a NIT, and “media or information” which “has been concealed through technological means” would apply to the IP addresses hidden by the Tor network. However, this subsection was not a part of Rule 41(b) at the time the NIT warrant was issued in the Playpen case. This subsection did not become effective until December 1, 2018.

85. Id.
86. See id.
87. See id.
88. See FED. R. CRIM. P. 41(b)(6).
89. Id.
91. FED. R. CRIM. P. 41(b)(6).
The question of whether this amendment will apply to past cases presents a more difficult issue, which will be discussed later in this Comment.\(^9^4\)

C. The Good Faith Exception

In *Weeks v. United States*\(^9^5\), the Supreme Court created what is now known as the exclusionary rule, holding that evidence seized in violation of the Fourth Amendment cannot be used in court against a defendant.\(^9^6\) Decades later in *United States v. Leon*\(^9^7\), the Supreme Court recognized the need for an exception to the exclusionary rule where officers reasonably relied on magistrate judges’ findings of probable cause.\(^9^8\) In *Leon*, police officers reasonably relied on a magistrate judge’s finding of probable cause in executing a search warrant, though the District Court ultimately found that probable cause did not exist under the circumstances upon which the warrant was based.\(^9^9\) The Supreme Court noted that the exclusionary rule was not part of the Fourth Amendment and was rather a “judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect.”\(^1^0^0\) Under the good faith exception, suppression is warranted only if an officer was reckless in drafting an affidavit, or if an officer could not have harbored a reasonable belief in the magistrate judge’s finding of probable cause.\(^1^0^1\)

D. Cases Rejecting the NIT Warrant

Several courts have rejected the NIT warrant because they found that it did not satisfy Rule 41(b) and that the good faith exception did not apply.\(^1^0^2\) In *United States v. Levin*\(^1^0^3\), which has since been vacated by the First Circuit, the District of Massachusetts...
setts held that the NIT warrant violated Rule 41(b).\textsuperscript{104} For purposes of 41(b)(1), the court was not persuaded by the argument that the server was located in the Eastern District of Virginia.\textsuperscript{105} The court said this argument was “immaterial, since it is not the server itself from which the relevant information was sought.”\textsuperscript{106} Likewise, the court rejected the government’s argument regarding Rule 41(b)(2), saying that the property to be searched was the computers outside the district.\textsuperscript{107} Lastly, the District of Massachusetts was not persuaded that the NIT was similar to a tracking device and refused to find that the NIT warrant satisfied Rule 41(b)(4).\textsuperscript{108}

Not only did the District of Massachusetts in Levin find that the warrant violated Rule 41(b), but it also refused to apply the good faith exception.\textsuperscript{109} The Levin court found that the warrant was void ab initio\textsuperscript{110} because the issuing court lacked jurisdiction.\textsuperscript{111} The Levin court noted that the Supreme Court has yet to apply the good faith exception to a case involving a warrant that was void ab initio.\textsuperscript{112} Ultimately, the Levin court found that the good faith exception does not apply where a warrant is void ab initio and granted the motion to suppress.\textsuperscript{113} However, the First Circuit has since vacated this decision, finding that the good faith exception does apply.\textsuperscript{114} Other than acknowledging the district court’s argument, the First Circuit did not otherwise comment on the whether the warrant at issue was void ab initio.\textsuperscript{115}

The District of Massachusetts was one of the first courts to grant a motion to suppress evidence obtained through the NIT warrant, but subsequent to the District of Massachusetts’s decision in Levin, other courts similarly granted motions to suppress.\textsuperscript{116} The

\begin{itemize}
  \item \textsuperscript{104} Id. at 34.
  \item \textsuperscript{105} Id.
  \item \textsuperscript{106} Id.
  \item \textsuperscript{107} Id.
  \item \textsuperscript{108} Id.
  \item \textsuperscript{109} Id. at 41–42.
  \item \textsuperscript{110} Ab initio means “from the beginning.” \textit{Ab initio}, \textsc{Black’s Law Dictionary} (10th ed. 2014).
  \item \textsuperscript{111} Levin, 186 F. Supp. 3d at 32.
  \item \textsuperscript{112} Id. at 39 (“None of the Supreme Court’s post-\textit{Leon} good faith cases, however, involved a warrant that was void \textit{ab initio}.”).
  \item \textsuperscript{113} Id. at 35.
  \item \textsuperscript{114} United States v. Levin, 874 F.3d 316, 324 (1st Cir. 2017) (“The district court erred in granting the motion to suppress. Because the executing officers acted in good faith reliance on the NIT warrant, the Leon exception applies. Accordingly, the district court’s order is vacated, and the case is remanded for further proceedings not inconsistent with this opinion.”).
  \item \textsuperscript{115} Id. at 321.
  \item \textsuperscript{116} See United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *22 (N.D. Okla. Apr. 25, 2016) (finding that the NIT Warrant
Northern District of Oklahoma cited *Levin* in support of granting a motion to suppress. The District of Colorado also cited *Levin* in support of suppression, only to be reversed later by the Tenth Circuit Court of Appeals. The District of Colorado followed *Levin* in finding that the good faith exception does not apply when a warrant is void ab initio.

### E. Cases Upholding the NIT Warrant

The district courts that have confronted cases involving the NIT warrant have not yet reached a consensus; however, an apparent majority has denied the motions to suppress. Also, the First, Tenth and Eight Circuits have denied motions to suppress. Most courts have denied the motions for one of two reasons: either the court finds that the warrant did not violate Rule 41(b), or the court finds that the warrant did violate Rule 41(b) but finds that suppression is not appropriate because the agents acted in good faith.

In *United States v. Matish*, the Eastern District of Virginia found that Rule 41(b)(4), the exception for tracking devices, authorized the NIT warrant. The court reasoned that the NIT was violated Rule 41(b) because it did not satisfy any of the subsections.}

---

117. *Arterbury*, 2016 U.S. Dist. LEXIS 67091, at *35 (granting a motion to suppress after finding that the warrant was void ab initio).
118. United States v. Workman, 205 F. Supp. 3d 1256, 1261-62 (D. Colo. 2016) (finding that the NIT Warrant did not fall into subsections one or two of Rule 41(b)), rev’d, 863 F.3d 1313 (10th Cir. 2017).
119. *Id.* at 1267 (“Because a warrant that was void at the outset is akin to no warrant at all, cases involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially instructive.”) (quoting United States v. Levin, 186 F. Supp. 3d 26, 41 (D. Mass. 2016) vacated, 874 F.3d 316 (1st Cir. 2017)).
121. As discussed, the First Circuit vacated the District of Massachusetts in United States v. Levin, 874 F.3d 316, 324 (1st Cir. 2017). The Tenth Circuit Court of Appeals reversed the District of Colorado in United States v. Workman, 863 F.3d 1313 (10th Cir. 2017), applying the good faith exception and denying the motion to suppress. The Eight Circuit Court of Appeals also denied suppression in United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017).
125. *Id.* at 612.
analogous to a tracking device and by accessing the website, the suspects made a “virtual trip” to the Eastern District of Virginia where the server was located.\footnote{126} 

Shortly before deciding \textit{Matish}, the Eastern District of Virginia found in \textit{United States v. Darby}\footnote{127} that the NIT warrant was authorized by the exception for tracking devices.\footnote{128} Also, the Eastern District of Wisconsin in \textit{United States v. Epich}\footnote{129} found that the warrant was authorized under Rule 41(b).\footnote{130} Notably, the Eastern District of Virginia in \textit{Darby} and the Eastern District of Wisconsin in \textit{Epich} referred to the text of the new subsection of Rule 41(b) in their opinions.\footnote{131} Although the new subsection was not in effect until December of 2016, the courts believed it was evidence of Congress’s intent to broaden the reach of magistrate judges’ authority under Rule 41(b).\footnote{132} 

The District Court for the Western District of Washington took a slightly different approach in \textit{United States v. Michaud},\footnote{133} finding that the warrant violated the “letter” but not the “spirit” of Rule 41.\footnote{134} In other words, the court acknowledged Congress’s intent to authorize a search like the one using the NIT warrant, but because the plain language of the Rule 41 in 2015 did not explicitly authorize such a search, the court could not find that the warrant was authorized by the Rule as it was written at the time.\footnote{135} 

Although courts have been hesitant to find that the February 2015 version of Rule 41(b) authorized the warrant, courts have been equally hesitant to allow suppression of the fruits of this warrant.\footnote{136} The court in \textit{Michaud} found that the NIT warrant violated

\footnotesize{
126. \textit{Id.} at 613 ("Accordingly, when users entered Playpen, they came into Virginia in an electronic manner, just as the police in \textit{Kyllo} entered a home in an electronic manner." (citing \textit{Kyllo} v. United States, 553 U.S. 27 (2001))).  
128. \textit{Id.}  
130. \textit{Id.}  
131. See \textit{Darby}, 190 F. Supp. 3d at 536; see also \textit{Epich}, 2016 WL 953269, at *2.  
132. See \textit{Darby}, 190 F. Supp. 3d at 536 ("The government characterizes this amendment as clarifying the scope of Rule 41(b), and this Court agrees."); see also \textit{Epich}, 2016 WL 953269, at *2 ("Judge Jones noted, as an aside, that the Supreme Court currently was reviewing a proposed amendment to Rule 41 that would address this very issue.").  
134. \textit{Id.} at *6.  
135. \textit{Id.} ("The Court must conclude that the NIT Warrant did technically violate Rule 41(b), although the arguments to the contrary are not unreasonable and do not strain credulity.").  
the letter of Rule 41(b), but nonetheless upheld the warrant under the good faith exception.\textsuperscript{137} Also, the Eastern District of Pennsylvania in \textit{United States v. Werdene}\textsuperscript{138} held that the warrant violated Rule 41(b) because it did not fit into any of the subsections.\textsuperscript{139} However, the court applied the good faith exception because “[a] magistrate judge’s mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression.”\textsuperscript{140} In \textit{Werdene}, the court addressed at length the errors it believed the District of Massachusetts made in \textit{Levin} in refusing to apply the good faith exception.\textsuperscript{141} The \textit{Werdene} court particularly noted that the \textit{Levin} court failed to weigh the costs of suppression.\textsuperscript{142} The subsequent criticism of \textit{Levin} appears to have led to change, as the District Court for the District of Massachusetts has more recently found that the good faith exception did apply to the NIT warrant.\textsuperscript{143}

In \textit{United States v. Anzalone},\textsuperscript{144} a different judge on the U.S. District Court for the District of Massachusetts—the same court that decided \textit{Levin}—found that the warrant was not void ab initio.\textsuperscript{145} In fact, the court followed the reasoning of other district courts and opined that even if the warrant was void ab initio, suppression was still not warranted because the good faith exception applied.\textsuperscript{146}

Several new arguments are emerging regarding the proposed amendment and the good faith exception. Defendants in numerous cases have argued that the good faith exception should not apply in the Playpen case because the agents should have known the warrant was invalid.\textsuperscript{147} However, the Middle District of Florida in

\textsuperscript{137} Michaud, 2016 WL 337263, at *7.
\textsuperscript{139} Id. at 442.
\textsuperscript{140} Id. at 453.
\textsuperscript{141} Id. at 450–51.
\textsuperscript{142} The Eastern District of Pennsylvania listed costs such as loss of trustworthy evidence. \textit{Id.} at 452 (“The court in \textit{Levin} did not analyze the ‘costs’ associated with suppression. The Supreme Court has stated that these costs are ‘substantial.’” (quoting United States v. Leon, 468 U.S. 897, 922 (1984))).
\textsuperscript{145} Id. at 372.
\textsuperscript{146} Id. (citing United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016)).
United States v. Adams\textsuperscript{148} believed that the warrant does not fall into the category of warrants that are so defective that the agents could not reasonably rely on them.\textsuperscript{149} Also, the court believed it is unfair to assume that the entire Department of Justice, including investigators, had the same knowledge as Assistant U.S. Attorneys regarding what constitutes probable cause.\textsuperscript{150} Courts cannot expect law enforcement to understand the complexities of a law and its amendments, and the court found that agents in the Playpen case were correct to rely on the magistrate judge’s authorization of the warrant.\textsuperscript{151}

F. The Possibility of Retroactivity

One important consideration of Rule 41(b) is whether the new subsection will be retroactive. If the recent amendment to Rule 41(b) is retroactive, the new subsection will apply to cases pending on direct review.\textsuperscript{152} At least one court, the District of North Carolina, has already found that the 2016 amendment does not apply retroactively.\textsuperscript{153} As discussed, the new subsection allows law enforcement to “use remote access” to search for electronically stored information “located within or outside that district” in cases where that information “has been concealed through technological means.”\textsuperscript{154}

Several of the district court decisions have already been appealed to the circuit courts.\textsuperscript{155} The circuit courts would have to apply this new subsection of Rule 41(b) if the Rule is retroactive.\textsuperscript{156}

\textsuperscript{148} Adams, 2016 WL 4212079, at *8.
\textsuperscript{149} Id.
\textsuperscript{150} Eure, 2016 WL 4059663, at *9.
\textsuperscript{151} Id.
\textsuperscript{152} See Griffith v. Kentucky, 479 U.S. 314, 322–23 (1987) (“But after we have decided a new rule in the case selected, the integrity of judicial review requires that we apply that rule to all similar cases pending on direct review.”).
\textsuperscript{154} Where the 2016 amendments to the Federal Rules of Criminal Procedure do not purport to apply retroactively, and where the current Rule 41(b) clearly does not embrace a Constitutional right that pre-exists the 2016 amendments, the analysis that follows evaluates the validity of the NIT warrant under the Rules in effect February 20, 2015. See also United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017) (applying Rule 41 as it was written in February 2015).
\textsuperscript{155} See supra note 152.
The “plain language” in Rule 41(b)(6) is fairly clear: magistrate judges are allowed to issue warrants outside their districts in exactly the type of situation presented in the Playpen cases. In the NIT warrant cases, the IP addresses of the perpetrators accessing Playpen were concealed through the Tor Network, and the NIT utilized remote access to attach to computers outside the Eastern District of Virginia.

Whether the proposed amendment will apply retroactively is less clear. In Griffith v. Kentucky, the Supreme Court held that “[a] new rule for the conduct of criminal procedure . . . applies retroactively to all cases, state or federal, pending on direct review or not yet final.” In doing so, the Court declined to follow the “clear break” rule, which states that a constitutional rule applies retroactively only when it represents a clear break from past precedent. In later cases, the Court specified that retroactivity applies when the new rule is substantive in nature and not merely procedural. As to what makes a rule substantive in nature, the Court has said that the rule must be one “without which the likelihood of an accurate conviction is seriously diminished.” A rule is substantive if it “alters the range of conduct of the class of persons that the law punishes.” Whether the new amendment applies retroactively will greatly impact the fate of the Playpen cases moving forward on appeal, as later sections of this Comment will discuss.

159. Id. at 363.
161. Id.
163. Griffith, 479 U.S. at 326.
165. Id. at 352 (quoting Teague v. Lane, 489 U.S. 288, 313 (1989)).
166. Id. at 353.
167. The Supreme Court in Teague declined to extend the rules regarding retroactivity to cases on collateral review rather than direct review. See Teague, 489 U.S. 288.
168. See infra Part III.A.
III. **Analysis**

**A. The Changes to Rule 41(b) Most Likely Do Not Apply Retroactively**

When defendants around the country began challenging the NIT warrant, one argument many of them raised was that the violation of Rule 41(b) was constitutional in nature, therefore leading to prejudice that would weigh in favor of suppression.\(^{169}\) Most courts to consider this challenge found that Rule 41(b) is procedural in nature and not constitutional or substantive.\(^{170}\) This characterization, although not helpful in determining whether the warrant itself is valid, is helpful in determining the retroactivity implications of the amendment to Rule 41(b). Because the majority of courts have found that a failure to comply with Rule 41(b) produces a “technical violation,”\(^{171}\) the Rule is most likely not constitutional in nature.

The nature of the Rule also indicates that it is procedural. The Rule does not make certain conduct criminal or not criminal.\(^{172}\) The Rule also does not extend criminal punishment to a new class of people.\(^{173}\) Rather, Rule 41(b) governs the authority over magistrate judges to issue warrants; an amendment to this Rule merely expands the “manner of determining the defendant’s culpability.”\(^{174}\) Therefore, the Rule does not affect the substantive nature of any crime and therefore does not apply retroactively.

On the other hand, the District of Massachusetts in *Levin* found that the Rule 41(b) violation was constitutional in nature and not procedural.\(^{175}\) The *Levin* court reasoned that Rule 41 as a whole has both substantive and procedural provisions and that subsection (b) is a substantive provision.\(^{176}\) The *Levin* court cited cases

\(^{169}\) See United States v. Levin, 186 F. Supp. 3d 26, 35-36 (D. Mass. 2016), **vacated**, 874 F.3d 316 (1st Cir. 2017) (discussing the nature of the violation and arguing that it is substantive in nature).

\(^{170}\) See United States v. Matish, 193 F. Supp. 3d 585, 622 (E.D. Va. 2016) (holding that the violation was not substantive because it did not violate defendant’s Fourth Amendment rights); see also United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016).

\(^{171}\) *Michaud*, 2016 WL 337263, at *6 (“[T]he NIT Warrant did not fail for constitutional reasons, but rather was the product of a technical violation of Rule 41(b).”).

\(^{172}\) As discussed earlier, Rule 41(b) involves the authority for magistrate judges to issue warrants. The rule does not reach the substance of specific crimes. Fed. R. Crim. P. 41(b)(6). See supra Part II.B.2.

\(^{173}\) See Fed. R. Crim. P. 41(b)(6).

\(^{174}\) Schiro v. Summerlin, 542 U.S. 348, 353 (2004) (noting that rules pertaining to the “manner of determining defendant’s culpability” are procedural and not substantive) (emphasis omitted).


\(^{176}\) Id.
holding that Rule 41(b) is constitutional, noting that subsection (b) is “unique from other provisions of Rule 41.” ¹⁷⁷

Though the possible retroactivity of Rule 41(b)(6) is not settled, the Rule most likely does not apply retroactively. The new subsection does not extend the class of persons punished because it discusses only the authority of magistrate judges. ¹⁷⁸ The Rule also does not affect the substantive nature of a crime because it does not discuss specific crimes at all; therefore, the rule is procedural. As discussed in the previous section, the Eastern District of North Carolina has already found that the new amendment does not apply retroactively; ¹⁷⁹ for the reasons stated above, other courts should find that the Eastern District of North Carolina is correct and the amendment does not apply retroactively.

B. Denying Suppression Is Consistent with the Spirit but Not the Letter of Rule 41(b)

Denying suppression of evidence gathered through these NIT warrant searches is most consistent with Rule 41(b); as such, many courts have denied suppression either by upholding the warrant or applying the good faith exception. ¹⁸⁰ The arguments that the warrant did not satisfy Rule 41(b) are persuasive because they are more consistent with the plain language of the Rule. The first five subsections do not describe the use of “remote access.” ¹⁸¹ Nonetheless, the good faith exception should apply because the agents justifiably relied on the warrant issued by the magistrate judge and should not be penalized for the magistrate judge’s mistake. ¹⁸²

Given the plain language of Rule 41(b) at the time the NIT warrant was issued, the NIT warrant in the Playpen case most likely was not authorized by any subsection in Rule 41(b). Though several courts have found that the NIT warrant was akin to a tracking device and therefore authorized under Rule 41(b)(4), ¹⁸³ at least one

¹⁷⁷ See United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (quoting United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008)).
¹⁸³ See Matish, 193 F. Supp. 3d at 612.
other court has criticized such a reading of Rule 41.\textsuperscript{184} Comparing the NIT to a tracking device is, as some courts have pointed out, a stretch of logic.\textsuperscript{185} Congress most likely meant Rule 41(b)(4) to authorize physical tracking devices, like the GPS used in the \textit{Jones}\textsuperscript{186} case, and not a device like the NIT. Also, Congress would not have amended the Rule had Congress already authorized warrants like the NIT warrant; Congress would not have needed to take action.\textsuperscript{187} Therefore, the majority position, that Rule 41(b) did not authorize the warrant, is most consistent with the plain language.

Although the previous version of Rule 41(b) did not explicitly authorize the use of a device like the NIT, subsection six would plainly authorize a device like the NIT.\textsuperscript{188} As discussed earlier, this subsection allows a magistrate judge to issue a warrant to use “remote access” when the district where the information is stored has been “concealed by technological means.”\textsuperscript{189} Therefore, if section six applies retroactively, Rule 41(b) would almost certainly authorize the Playpen warrant.\textsuperscript{190} Assuming that Rule 41(b) does not apply retroactively for the reasons stated in the previous section,\textsuperscript{191} Rule 41(b) does not plainly authorize the use of the NIT warrant.\textsuperscript{192}

Nevertheless, despite violating the plain language of Rule 41(b), suppression is still not appropriate. The fact that Congress later authorized the exact type of warrant in this case shows that

\textsuperscript{184} See Michaud, 2016 WL 337263, at *6 (finding flaw in the tracking device analogy since installation either occurred on the government computer, which was never controlled by the defendant, or the defendant’s computer, which was never located in the Eastern District of Virginia); see also United States v. Anzalone, 208 F. Supp. 3d 358, 370 (D. Mass. 2016) (finding that the NIT was not akin to a tracking device).

\textsuperscript{185} See Michaud, 2016 WL 337263, at *6.

\textsuperscript{186} United States v. Jones, 565 U.S. 400, 403 (2012).

\textsuperscript{187} See United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108, at *6 (N.D. Cal. Sept. 1, 2016) (“Henderson argues that because it proposed this amendment, the government was well aware that Rule 41(b), as it stands, does not authorize the type of search conducted by the NIT Warrant.”).

\textsuperscript{188} United States v. Eure, No. 2:16CR43, 2016 WL 4059663, at *9 (E.D. Va. July 28, 2016) (finding that the proposed amendment “explicitly authorize[s]” this type of search); see also Owsley, supra note 3, at 315–16 (“Recently, the Department of Justice proposed a change to Rule 41 to authorize search warrants for Trojan devices in all types of criminal investigations.”).

\textsuperscript{189} \textsc{Fed. R. Crim. P.} 41(b)(6).

\textsuperscript{190} See Owsley, supra note 3, at 315–16.

\textsuperscript{191} \textit{Supra} Part IIA.

\textsuperscript{192} This is the position of most courts that have considered this issue. See United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016); see also United States v. Werdene, 188 F. Supp. 3d 431, 440 (E.D. Pa. 2016) (“[T]he courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant.”).
Congress intended the Rule to allow this type of search. Further, the agents took steps beyond what may have been necessary. It is unclear whether the use of the NIT was even a Fourth Amendment search, meaning the agents who applied for the warrant were being cautious. Overall, the NIT warrant cases present situations where the good faith exception is critical. Given that the NIT warrant followed the spirit of the law, the agents had every reason to believe the warrant was legitimate. Therefore, this situation is not one in which the harsh consequences of suppression are justified.

C. Policy Arguments in Favor of Denying Suppression

Issues of government surveillance present a delicate situation where a court must weigh privacy interests against the importance of the government’s ability to detect crime and protect the public. At least one court found it necessary to discuss the policy behind its decision regarding the Playpen warrant. The Matish court acknowledged the need to consider privacy interests, but ultimately found that the need for government surveillance outweighed privacy interests. The Matish court noted the “especially pernicious nature of child pornography” and the “continuing harm to the victims” as part of its reasoning. Notably, the court also discussed the technological race between the government and

193. This is the argument put forth in Darby. United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016). This argument does make it clearer that the warrant violated the plain language but also that it followed the spirit of the law. Id.

194. United States v. Matish, 193 F. Supp. 3d 585, 621 (E.D. Va. 2016) (finding that the government did not even need a warrant to use the NIT).


196. Matish, 193 F. Supp. 3d at 621 (“T]he Court recognizes the need to balance an individual’s privacy in any case involving electronic surveillance with the Government’s duty of protecting its citizens.”); see Devin M. Adams, The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, “Particularly” Speaking, 51 U. RICH. L. REV. 727, 745-49 (2017) (discussing the controversial process of introducing the amendment to Rule 41(b), due to its expansion of government power to search remotely); see also Zach Lerner, A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 YALE J. L. & TECH. 26, 69 (2016) (“Although the amendments to Rule 41 merely seek to extend extraterritorial warrant authority to two emerging cybercrimes, these changes, if unchecked, could effectively transform remote access search warrants into ubiquitous surveillance tools.”).

197. See Matish, 193 F. Supp. 3d at 621.

198. Id.

199. Id.
criminals attempting to access child pornography. As the Matish court indicated, “[t]he Government’s efforts to contain child pornographers, terrorists and the like cannot remain frozen in time.” The Matish court decided that the government should be given some leeway to detect criminal activity, even if that involves acting on a warrant issued out of the jurisdiction.

The policy arguments set forth in Matish deserve some further consideration. One policy argument in favor of the defense is that government surveillance could interfere with innocent third parties. However, it seems that in the Internet age, jurisdiction as well as privacy are slowly eroding. Just as the expectation of privacy test in Katz v. United States is becoming less effective now that information is routinely stored on the Internet in the control of third parties, geographic jurisdiction appears to be less relevant. This lack of relevance is due in part to the fact that the Internet itself is an undefined, non-geographic location.

The amendment to Rule 41(b) demonstrates Congress’s acknowledgment of the trend towards erosion of traditional geographic jurisdiction because it gives magistrate judges even more power to issue warrants outside the district.

200. Id.
201. Id.
202. Id.
203. See Owsley, supra note 3, at 315, 317 (using the example of parents being apprehended for the criminal conduct of their children on the home computer); see also Lerner, supra note 196, at 55 (“[T]he amendments may adversely affect Internet infrastructure, causing disruption to innocent third parties.”).


206. See United States v. Perrine, 518 F.3d 1196, 1204 (2008) (“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.” (citing Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001))).


208. Id. at 1370; see supra Part I.B (discussing Rule 41(b) and the various ways in which magistrate judges can exercise authority outside their jurisdictions).

209. The amendment allows for the use of “remote access” and is one of five subsections that allow for magistrate judges to issue warrants affecting persons or property outside their jurisdictions. See Fed. R. Crim. P. 41(b).
Where some might look at the new concept of jurisdiction skeptically, Matish highlights the rationale for giving more deference to the government in its investigation of criminal activity. Judges should take caution to not inadvertently allow the government to access information belonging to innocent third parties. However, regardless of the risk to third parties in the government’s quest for seeking out criminals, the court in Matish correctly found that public safety is too valuable and outweighs potential infringements of third-party privacy in the context of eliminating child pornography.

D. Possible Ways to Ensure Magistrate Judges Do Not Overstep Jurisdictional Boundaries

Another question that remains is what courts should do with the evidence produced from the Playpen warrant once it has been seized illegally. Most courts faced with challenges to the NIT warrant have dealt with them in the context of granting or denying motions to suppress. Ever since its adoption in Weeks, the exclusionary rule has been controversial. The aim of the exclusionary rule, as discussed in the previous section, was originally both deterrence of police misconduct and preservation of the integrity of the judicial system. With the adoption of the good faith exception, the Court appeared to affirm that deterrence is the main justification for the exclusionary rule, if not the only justification for it.

211. Supra Owsley, note 3, at 315, 347 (“There is a danger that [Trojan devices] will collect information not meant to be obtained from innocent third parties.”).
212. See Matish, 193 F. Supp. 3d at 621–22.
213. See United States v. Werdene, 188 F. Supp. 3d 431, 439 (E.D. Pa. 2016) (considering defendant’s motion to suppress evidence seized from his home); see also Matish, 193 F. Supp. 3d at 592 (considering defendant’s motion to suppress evidence seized from his home computer); United States v. Anzalone, 208 F. Supp. 3d 358 (D. Mass. 2016) (considering defendant’s motion to suppress evidence gathered by the NIT search).
214. See Eugene Milhizer, The Exclusionary Rule Lottery Revisited, 59 CATH. U. L. REV. 747 (2010) (discussing the history of the exclusionary rule and how it can be made better); see also Kit Kinports, Culpability, Deterrence, and the Exclusionary Rule, 21 WM. & MARY BILL RTS. J. 821 (2013) (discussing the lack of clarity in case law regarding the exclusionary rule).
215. Supra Part II.C.
Deterrence in the form of excluding evidence has little effect in the area of issuing warrants. For purposes of federal crimes, magistrate judges are entrusted with the authority to issue warrants based on a determination of probable cause. A magistrate judge’s position is one of impartial neutrality, therefore, magistrates have no incentive to issue warrants that are faulty or lack probable cause. For this reason, the judicial system trusts magistrate judges with the responsibility to issue warrants rather than relying on law enforcement. As the Supreme Court has said, “the whole point of the [exclusionary] rule . . . is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations.” Unfortunately, the exclusionary rule then does little to deter magistrate judges. Because they are inherently impartial, magistrate judges have nothing to lose from issuing faulty warrants. The Court created the good faith exception based on the idea that law enforcement officers should not be punished for mistakes made by magistrate judges.

Given that the exclusionary rule has been associated with “substantial social costs,” it may be time to begin looking for a new solution that will better serve the goals of the Fourth Amendment. In particular, magistrate judges should be given more of an incentive to not issue warrants out of their jurisdictions. The current exclusionary rule assumes magistrate judges have no incentive to issue faulty warrants, but magistrate judges also have little incentive to issue proper warrants because there are few consequences if they fail to do so. One potential means to incentivize proper issuance of warrants is to revise the Code of Judicial Conduct to make it

218. See id. at 917.
221. See Leon, 468 U.S. at 917 (“Judges and magistrates . . . have no stake in the outcome of particular criminal prosecutions.”).
223. See Leon, 468 U.S. at 917 (“The threat of exclusion thus cannot be expected significantly to deter [magistrate judges].”).
224. See id.
225. See id. The Court did leave open the possibility that if the magistrate judge has “abandoned his detached and neutral judicial role,” suppression may be appropriate. Id. at 926.
226. See Hudson v. Michigan, 547 U.S. 586, 591 (2006) (discussing the fact that the court has tried to narrow the scope of the exclusionary rule because it can result in letting the guilty go free).
227. See supra note 221.
228. See George R. Nock, The Point of the Fourth Amendment and the Myth of Magisterial Discretion, 23 Conn. L. Rev. 1, 9 (1990) (“It is hard to imagine a judge suffering at the polls for a tendency to issue too many warrants that have uncovered evidence of criminal conduct.”).
clearer that magistrates are not allowed to issue warrants that clearly go beyond their jurisdictional authority and hence are void ab initio. By putting a provision in the Code of Judicial Conduct, judges will have more of an incentive to ensure the warrants they issue do not exceed their jurisdictional authority as set forth in the Federal Rules of Criminal Procedure. Even as recent amendments expand this very authority, the lack of safeguards to ensure their compliance with the rules is alarming.229

E. The New Subsection and the Good Faith Exception

The majority of courts have “saved” the NIT warrant on the good faith exception alone.230 As discussed, many courts have found that while the warrant violated the plain language of Rule 41(b), suppression is not justified.231 Some defendants have refused to believe that the officers could have relied on the warrant.232 In doing so, they invoke an exception to the exception: officers cannot be said to have relied in “good faith” on a warrant that is “so facially deficient” that an officer cannot reasonably rely on it.233 Law enforcement officers are expected to have some understanding of the law, but they cannot be expected to have the same degree of knowledge as those practicing law.234 Therefore, depending on whether the NIT warrant was “facially deficient” in light of the amendment to Rule 41(b), the good faith exception may or may not apply.

229. Even though Rule 41(b) explicitly allows the type of extraterritorial search in this case, some have still suggested modifying the amendments to mandate additional disclosure of the technical process the government plans to use to obtain information outside its jurisdiction. See Lerner, supra note 196, at 67–68. The hope is that adding this requirement would provide the judiciary with greater transparency and mitigate harm to third parties. Id. at 67.


231. See Werdene, 188 F. Supp. 3d at 448; see also Henderson, 2016 WL 4549108, at *4.


234. Eure, 2016 WL 4059663, at *9 (“Defendant seeks to attribute to the FBI agents that sought the warrant the legal expertise of the DOJ lawyers but nothing indicates that these agents knew that the warrant might violate Rule 41(b).”).
The addition of this new subsection has led to several vastly different viewpoints. At least one defendant has argued that the amendment shows that Rule 41(b) could not have applied in this situation. The amendment, in other words, makes it clearer that Rule 41(b), as it read in February 2015, did not allow this type of search. Congress added something new to the Rule; it would not have done so had the Rule already permitted a magistrate judge to issue a warrant to use a device such as a NIT. Still, many of the district courts that have considered this issue believe that knowledge of the proposed amendment and the potential effects on the law is beyond the scope of what an ordinary law enforcement officer is expected to know.

Although law enforcement officers often have to make quick determinations on legal issues such as probable cause, Rule 41(b) concerns the authority of magistrate judges rather than the Fourth Amendment. Officers are therefore less likely to be aware of nuanced interpretations of this rule the same way they are aware of Fourth Amendment interpretations. Furthermore, the confusion that the amendment has caused courts shows that the Rule’s application is less than clear. If the courts cannot agree on whether this particular warrant violates Rule 41(b), law enforcement could not reasonably be aware that the warrant violated the Rule. Since the majority position is that the good faith exception applies,

236. Id.
237. Eure, 2016 WL 4059663, at *9 (“[T]he Department of Justice (“DOJ”) had been seeking to amend Rule 41(b) to explicitly authorize this type of warrant.”).
238. See Henderson, 2016 WL 4549108, at *6 (“Henderson argues that because it proposed this amendment, the government was well aware that Rule 41(b), as it stands, does not authorize the type of search conducted by the NIT Warrant.”).
239. See id.; see also Eure, 2016 WL 4059663, at *9.
242. See Henderson, 2016 WL 4549108, at *6 (“[A] single court’s decision analyzing a complicated and ‘novel request’ does not definitively demonstrate that the FBI deliberately disregarded the Rule. Indeed, multiple courts have now found that the NIT Warrant is valid under Rule 41.”).
it seems likely that courts will continue to uphold the warrant under the good faith exception.

IV. CONCLUSION

The growing use of the Internet as a forum for criminal activity has led to the use of creative techniques for criminal detection, some of which have caused interesting legal dilemmas. The use of the Tor Network for criminal activity, such as child trafficking and child pornography, leaves the government in a position where it must either invade the privacy of its citizens through the use of Trojan devices, or allow heinous crime to go undetected. Not only is the government in a difficult position in having to choose safety over privacy, but unclear rules have made it more difficult for law enforcement to do its job and stop criminal activity. Luckily, Congress has amended the Federal Rules of Criminal Procedure to make it clearer when magistrate judges can issue warrants outside of their districts. In the meantime, it is most consistent with public policy and the Court’s holding in Leon to admit the evidence retrieved by the NIT warrant in the Playpen cases.

Several questions regarding Rule 41(b) have yet to be definitively answered: does Rule 41(b) authorize the use of remote devices like the NIT? If not, does subsection six apply retroactively to the NIT warrant issued well over a year before the amendment went into effect? If either of these questions can be answered in the affirmative, then the NIT warrant is likely legitimate. Although the district courts do not agree on the answers to these questions, the Tenth, Eighth, and First Circuit Courts of Appeal have thus far denied motions to suppress. Most likely, courts

244. See Nakashima, supra note 2.
245. See Donohue, supra note 9, at 623.
246. See Matish, 193 F. Supp. 3d at 621-22.
249. See Eure, 2016 WL 4059663, at *8 (finding that the warrant did not violate Rule 41(b)); see also United States v. Levin, 186 F. Supp. 3d 26, 34 (D. Mass. 2016) vacated, 874 F.3d 316 (1st Cir. 2017) (finding that the magistrate judge lacked jurisdictional authority to issue the warrant under Rule 41(b)).
250. See Eure, 2016 WL 4059663, at *9 (discussing how the proposed amendment explicitly allows the type of search that occurred in this case).
251. The Tenth Circuit Court of Appeals reversed the District of Colorado in United States v. Workman, 863 F.3d 1313 (10th Cir. 2017), applying the good faith exception and denying the motion to suppress. The Eighth Circuit Court of Appeals in United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017), also denied suppression. Also, the First Circuit has vacated United States v. Levin, applying the good faith exception and denying suppression. United States v. Levin, 874 F.3d
confronted with NIT warrant cases moving forward will continue to follow the apparent-majority position of other districts and find that the NIT warrant was not explicitly authorized by Rule 41(b) as it was written prior to the December 2016 amendment.252

Even if the NIT warrant is not plainly authorized by the language of Rule 41(b), the good faith exception is a remedy that can, and should, be utilized. The exclusionary rule has long been used as a means of enforcing the Fourth Amendment by deterring unconstitutional police conduct and was not intended to influence magistrate judges’ conduct.253 However, the exclusionary rule has been criticized by many, including the Supreme Court itself, because the rule can result in setting criminals free on mere technicalities.254

In the Playpen case, the agents used the information available and obtained a search warrant, giving them what they believed to be authority to conduct the search.255 The NIT warrant authorized a search to collect information necessary to obtain probable cause for local search warrants of suspects’ homes in order to gather more evidence.256 Therefore, suppressing the evidence gathered from the original NIT warrant would force federal prosecutors around the country to drop charges because evidence more clearly establishing the guilt of these defendants would be suppressed.257 The policy arguments against suppression are numerous; in the interest of jus-


254. See Hudson v. Michigan, 547 U.S. 586, 591 (2006) (“The exclusionary rule generates ‘substantial social costs,’ . . . which sometimes include setting the guilty free and the dangerous at large.” (quoting Leon, 468 U.S. at 591)).

255. See Werdene, 188 F. Supp. 3d at 453 (“Once the warrant was issued, albeit outside the technical bounds of Rule 41(b), the agents acted upon an objectively reasonable good faith belief in the legality of their conduct.”).

256. See id. at 438–39 (stating that law enforcement detected defendant through monitoring the NIT); see also United States v. Matish, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016) (“Defendant seeks to suppress ‘all evidence seized from Mr. Matish’s home computer by the FBI on or about February 27, 2015 through the use of a network investigative technique, as well as all fruits of that search.’” (quoting Def.’s First Mot. to Suppress at 1)).

257. The doctrine of the “fruit of the poisonous tree” would effectively destroy the government’s case because if the evidence from the NIT warrant is suppressed, any subsequent warrants would lack probable cause. Wong Sun v. United States, 371 U.S. 471, 488 (1963) (holding that evidence discovered by law enforce-
tice, courts should apply the good faith exception and admit the evidence obtained from the NIT warrant.

The exclusionary rule is not a perfect remedy to the problem of enforcing the Fourth Amendment. As the NIT warrant cases show, the exclusionary rule fails to regulate magistrate judges’ conduct because they are inherently neutral. Therefore, in order to avoid the inequitable situation where the good faith exception constantly saves invalid warrants, there should be a new remedy. One possibility is to create a provision in the Judicial Code of Conduct that would prevent magistrate judges from issuing warrants outside of their districts when they are not authorized to do so. As the Internet continues to affect geographic jurisdiction, it will only become more necessary in the future to establish a way to prevent magistrate judges from unlawfully extending their jurisdictions, as was done in the Playpen case.

258. See Hudson, 547 U.S. at 591 (2006) (“Suppression of evidence, however, has always been our last resort, not our first impulse.”).

259. See supra note 223.