University of Baltimore Law Review

Volume 47 | Issue 3 Article 5

2018

NIT vs. Tor: A Struggle For The Right To Internet Anonymity

Richard E. Byrne III

NIT VS. TOR: A STRUGGLE FOR THE RIGHT TO INTERNET ANONYMITY

Richard E. Byrne III[*]

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[1]

I. INTRODUCTION

The Fourth Amendment of the United States 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.[2]

In other words, the government cannot search and seize people or their property without a valid warrant backed by probable cause.[3] Over the years, the advancement of technology has put the Fourth Amendment to the test, requiring the Supreme Court to clarify the law and the extent of both civilian rights and government powers time and time again.[4]

We live in a digital age. Not only do our lives revolve around technology, but so do the actions of criminals and police alike. As criminals find new ways to exploit technology, the law often struggles to keep up.[5] In some instances, modern technology may

---

* J.D. Candidate, May 2018, University of Baltimore School of Law; B.A., Jurisprudence, 2016, University of Baltimore. The author would like to specially thank the legendary Byron L. Warnken for his guidance and inspiration to him and countless others throughout the years; the Law Review staff for all their passion and devotion to their work; and his family for their undying love and support. The author dedicates this Comment to the memory of his father, Richard E. Byrne Jr. (1969–2018).

1. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).
2. U.S. CONST. amend. IV.
3. *Id.*
4. *See infra* Part III.
5. *See infra* Parts III–IV.

even find itself in a gray area of the law, where judges are left to apply—and often stretch—the law through their own interpretations.[6] Such interpretations may very well differ from one judge to another.[7]

A prime example of this conundrum is the FBI's recent acquisition of a child pornography website and the tactics used to uncover the identities of numerous patrons of the site.[8] Through the use of a network investigative technique (NIT)—a tool akin to malware—on the site's servers, the FBI could prompt users' computers to involuntarily send back identifying information that could be used to locate and arrest the users.[9] When the users were charged with possession of child pornography, many moved to suppress the evidence on the grounds that their Fourth Amendment rights were violated.[10] Because the defendants are from various states across the country, they challenged the authority of the Virginia magistrate to issue an NIT warrant that spanned the entire nation.[11] Accordingly, district courts across the nation have frequently come to different conclusions on this matter.[12] Due to the complexity of modern technology, the applicability of the Fourth Amendment has been questioned by many district courts, resulting in numerous conflicting decisions.[13] Whereas some courts have found the NIT's retrieval of identifying information to be a Fourth Amendment search, others have declined to do so, instead choosing to overlook the distinguishing facts and rely on prior case law which generally held that individuals have no expectation of privacy in such information.[14]

---

6. *See infra* Part III.
7. *See infra* Part IV.
8. United States v. Matish, 193 F. Supp. 3d 585, 594–96 (E.D. Va. 2016).
9. *Id.* at 594–95. The District Court for the Western District of Arkansas referred to NIT as malware, using the terms interchangeably. *See* United States v. Jean, 207 F. Supp. 3d 920, 927–29 (W.D. Ark. 2016). The court noted that the term "malware" means "malicious software." *Id.* at 927 n.7. Although Agent Alfin of the FBI objected to the term due to its "derogatory connotation," he conceded that the term is indeed descriptive of the NIT. *Id.*
10. *See, e.g.*, United States v. Broy, 209 F. Supp. 3d 1045, 1048, 1050 (C.D. Ill. 2016); United States v. Croghan, 209 F. Supp. 3d 1080, 1085 (S.D. Iowa 2016); United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *2 (W.D. Tex. Sept. 9, 2016); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016); *Matish*, 193 F. Supp. 3d at 592; United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *3 (W.D. Wash. Jan. 28, 2016).
11. *See* cases cited *supra* note 10.
12. *See* cases cited *supra* note 10.
13. *See infra* Part IV.
14. *See infra* Part IV.

This Comment will explore the incongruities between the decisions that arose as a result of this specific FBI operation and how the advancement of technology has fallen into a gray area of law where the applicability of our constitutional rights has come into question.[15] This will be achieved by first examining the events leading up to this issue.[16] This Comment will then explain how the advancement of technology in our society has shaped and evolved the Fourth Amendment throughout the years.[17] Next, it will explore how the courts have tackled this issue and where some went wrong.[18] Finally, the issue will be resolved by means of a *Katz* analysis of one's reasonable expectation of privacy in a Tor-concealed IP address, as well as through a recent amendment made by Congress to the preexisting law.[19]

II. FACTUAL HISTORY

The prosecution of numerous individuals was the result of the FBI's investigation of Playpen, a website that contained pornography.[20] The FBI was first alerted to the presence of Playpen in December 2014, when a foreign law enforcement agency discovered the site and subsequently informed the FBI.[21] The forum-style site was frequented by more than 150,000 total members and hosted "tens of thousands of postings related to child pornography."[22]

Playpen operated solely on "the onion router" or "Tor" network.[23] The Tor network was originally created by the United States Naval Research Laboratory for the purpose of protecting government communications.[24] The service is now publicly available from the "Tor Project" website, where anyone can download the Tor browser.[25] The use of the Tor network "allows users to access the Internet in an anonymous fashion" by concealing the user's Internet Protocol (IP) address from the sites he visits.[26] This is done by

15. *See infra* Parts III–IV.
16. *See infra* Part II.
17. *See infra* Part III.
18. *See infra* Part IV.
19. *See infra* Part V.
20. *See* United States v. Matish, 193 F. Supp. 3d 585, 593–94 (E.D. Va. 2016).
21. *Id.* at 594.
22. *Id.*
23. *Id.* at 593.
24. *Id.*
25. *Id.*
26. *Id.* at 593–94. An IP address is a unique identifying number given to every single device that connects to the Internet. Tim Fisher, *What Is an IP Address?*, LIFEWIRE

passing the user's IP address between various volunteer-operated "node" computers located around the world.[27] Furthermore, the Tor network also serves the secondary purpose of granting access to "hidden services," websites that can only be accessed via the Tor network.[28] Through the use of the Tor network, a hidden service website cannot locate its visitors, and vice versa.[29] As such, the Tor network is home to many illegal activities.[30] Given the illegal nature of the site, Playpen operated as one of these hidden services.[31]

The FBI located the individual operating Playpen and proceeded to execute a search of his home in Florida on February 19, 2015.[32] Rather than shutting Playpen down, the FBI assumed control and operated it from a government facility in the Eastern District of Virginia from February 20, 2015, through March 4, 2015.[33] At the start of the FBI's operation of Playpen, a federal magistrate judge in the Eastern District of Virginia authorized a search warrant.[34] This search warrant authorized the deployment of an NIT on Playpen's server "to obtain identifying information from activating computers."[35] The NIT consisted of computer code that was sent to the computer accessing Playpen and instructed it to send certain information to the FBI, unbeknownst to the computer's user.[36] The

(Jan. 17, 2018), https://www.lifewire.com/what-is-an-ip-address-2625920. It is a special serial number used as a tool for identification, akin to a car's license plate or a telephone number. *Id.* Internet authorities provide large amounts of IP addresses to regional Internet Service Providers (ISPs), which then assign the IP addresses to every server and Internet user. *See id.*

27. United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *1 (C.D. Cal. Aug. 8, 2016).
28. *Matish*, 193 F. Supp. 3d at 593.
29. *Id.* at 593–94.
30. *Id.* at 593.
31. *See id.* at 593–94.
32. *Id.* at 594.
33. *Id.* at 594; United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *1 (W.D. Wash. Jan. 28, 2016).
34. *Matish*, 193 F. Supp. 3d at 594; *Michaud*, 2016 WL 337263, at *2.
35. *Matish*, 193 F. Supp. 3d at 594. "Activating users" was defined in the warrant as computers "of any user or administrator who logs into [Playpen] by entering a username and password." *Id.* at 594–95 (alteration in original).
36. *Matish*, 193 F. Supp. 3d at 595; *Michaud*, 2016 WL 337263, at *2. The FBI declined to give defendants the complete source code to the NIT or provide additional information as to its operating parameters. *Matish*, 193 F. Supp. 3d at 596. The NIT is just one of many tools, or so-called "Trojan devices," used to combat illegal activity on the Tor network. *See* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 316 (2015). Other such tools include: "data extraction software, . . . port reader, harvesting program, remote search, CIPAV for

only information needed by the FBI to locate an activating computer was the IP address, which the government admittedly could not retrieve without deploying the NIT.[37]

After the NIT revealed a user's IP address, the FBI subpoenaed the users' Internet Service Provider (ISP) to obtain personal information regarding the individual's identity and address.[38] After this, the FBI then sought separate residential search warrants for the defendants' homes, seizing their computers, as well as other electronics and storage devices.[39]

Using this tactic, the FBI was able to locate numerous Playpen visitors so that they could be charged with crimes pertaining to child pornography.[40] However, many of these individuals filed motions to suppress evidence on the grounds that their Fourth Amendment rights against unreasonable searches and seizures were violated when the FBI executed the first search warrant that authorized the use of the NIT.[41] The defendants claimed that the NIT warrant was invalid, resulting in the constitutional equivalent of a warrantless search.[42]

While the reasons for alleging that the warrant was invalid vary between each of the cases, each court addressed the issue of whether the use of the NIT to retrieve an IP address even amounts to a search under the Fourth Amendment.[43] To understand how and why these courts were at odds with one another, it is imperative to understand how the constant development of technology has shaped the Fourth Amendment over the years, as well as the ways courts determine whether something is subject to Fourth Amendment protection.[44]

Computer and Internet Protocol Address Verifier, or IPAV for Internet Protocol Address Verifier." *Id.*

37. *Matish*, 193 F. Supp. at 595 (listing other information retrieved by the NIT, including: a "unique identifier generated by the NIT" assigned to each unique computer; the type, version, and architecture of the activating computer's operating system; information about whether the NIT has already been delivered to the activating computer; "the activating computer's Host Name"; "the activating computer's active operating system username"; and "the activating computer's media access control ('MAC') address").
38. *Id.* at 595–96.
39. *See id.* at 596.
40. *See* cases cited *supra* note 10.
41. *See* cases cited *supra* note 10.
42. *See* cases cited *supra* note 10.
43. *See* cases cited *supra* note 10.
44. *See infra* Parts III–IV.

III. THE TECHNOLOGICAL EVOLUTION OF THE FOURTH AMENDMENT

In the 1928 case of *Olmstead v. United States*, the Supreme Court adopted a physical trespass theory to determine whether the Fourth Amendment prohibition against unreasonable searches and seizures had been violated.[45] The Court held that wiretapping did not violate the Fourth Amendment because "[t]here was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[46]

Nearly four decades later, in *Katz v. United States*, the Supreme Court addressed the Fourth Amendment implications of eavesdropping via electronic surveillance.[47] While there was no Fourth Amendment violation under the physical trespass theory, the Court determined that the Government had constructively entered the Defendant's phone booth through the use of electronic surveillance.[48] The *Katz* Court believed the standard set in *Olmstead* was inadequate to provide protection against unreasonable searches and seizures.[49] Therefore, it adopted a new Fourth Amendment applicability test.[50]

The *Katz* test resolved the applicability of the Fourth Amendment based on whether the defendant had a "reasonable expectation of privacy."[51] This test, laid out in Justice Harlan's concurring opinion and first adopted in *Smith v. Maryland*,[52] relied on two components: one subjective, and the other objective.[53] The first was whether the defendant held a subjective expectation of privacy.[54] The second was whether society was willing to recognize that subjective expectation of privacy as being objectively reasonable.[55] Despite differing on the rationale, Justice Harlan agreed with the majority's holding that the defendant's Fourth Amendment rights had been violated when the Government intercepted his calls through the attachment of an eavesdropping device to a public telephone booth.[56] In its reasoning,

45. 277 U.S. 438, 463–66 (1928).
46. *Id.* at 464.
47. *See* 389 U.S. 347, 350, 353–54 (1967).
48. *Id.* at 353.
49. *Id.*
50. *See id.* at 351–53.
51. *Id.* at 360 (Harlan, J., concurring).
52. 442 U.S. 735, 740 (1979).
53. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
54. *Id.*
55. *Id.*
56. *Id.* at 360–61.

the Court noted that "the Fourth Amendment protects people, not places."[57]

The 2012 Supreme Court case of *United States v. Jones* involved the attachment of a GPS tracking device to a vehicle for four weeks without a valid warrant.[58] Prior case law held that there is no reasonable expectation of privacy in the exterior of one's vehicle when it is parked in a public place.[59] Despite the lack of a reasonable expectation of privacy, the Court in *Jones* still found the tracking of the defendant's vehicle to be a violation of his Fourth Amendment rights under the physical trespass theory.[60] The Court held:

> Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must "assur[e] preservation of that degree of privacy against [the] government that existed when the Fourth Amendment was adopted.". . . [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates. *Katz* did not repudiate that understanding.[61]

The Court explained that the *Katz* test did not replace the common-law trespassory test, but added to it instead.[62] It further explained, through the words of a prior opinion: "[W]e [do not] believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home . . . ."[63] The Court held that placing the GPS tracking device on the vehicle without a valid warrant violated the Fourth Amendment through the physical trespass theory.[64]

The Supreme Court case of *Kyllo v. United States* explored *Katz* in a modern sense and stressed the danger that the advancement of technology posed to our Fourth Amendment rights.[65] The Court tackled the issue of whether the use of thermal imaging technology that detected heat emanating from the exterior of one's home was

57. *Id.* at 351 (majority opinion).
58. 565 U.S. 400, 402–03 (2012).
59. *E.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983).
60. *Jones*, 565 U.S. at 404–05.
61. *Id.* at 406–07 (footnotes and citations omitted).
62. *See id.*
63. *Id.* at 407 (quoting Alderman v. United States, 394 U.S. 165, 180 (1969)).
64. *Id.* at 404–05.
65. 533 U.S. 27, 34 (2001).

considered a "search" under the Fourth Amendment.[66] The Court reasoned that the technology was used to gather information regarding the home's interior, and thus stated: "To withdraw protection of . . . [the] minimum expectation [of privacy within one's home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[67] Noticing that police technology poses a threat to an individual's reasonable expectation of privacy within their home, the Court held: "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[68]

In 2014, the Supreme Court held that police may examine the physical aspects of an arrestee's cell phone, but cannot conduct warrantless searches of the digital data within.[69] It reasoned that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[70] It further explained that the data within a cell phone warrants a degree of privacy, as it may contain personal communications, photos, Internet-searches of private interests or concerns, or even a person's specific movements—all over the course of an extended period of time.[71] The Court even noted that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[72]

The Supreme Court has consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.[73] A lack of expectation of privacy has been found in voluntarily-conveyed information such as numbers dialed on a phone,[74] bank account records,[75] tax records,[76] and oral

66. *Id.* at 29.
67. *Id.* at 34.
68. *Id.* at 40.
69. Riley v. California, 134 S. Ct. 2473, 2485 (2014).
70. *Id.*
71. *Id.* at 2490.
72. *Id.*
73. *See, e.g.*, Smith v. Maryland, 422 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–44 (1976); Couch v. United States, 409 U.S. 332, 335–36 (1973); United States v. White, 401 U.S. 745, 749, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963).
74. *Smith*, 422 U.S. at 743–44.
75. *Miller*, 425 U.S. at 442–44.
76. *Couch*, 409 U.S. at 335–36.

statements.[77] This rule has also been widely applied to IP addresses.[78] Courts in the Third, Seventh, and Tenth Circuits have held that sharing an IP address with a web service, such as an online chat service or email account, removes any expectation of privacy a person has in his IP address.[79] However, courts in the Ninth and Eleventh Circuits have taken it a step further by holding that an individual has no expectation of privacy in his IP address because he voluntarily shares that information with his ISP upon accessing the Internet.[80]

When looking back through the history and evolution of the Fourth Amendment, it is readily apparent that as technology advanced, there was a necessity for law to adapt and change along with it.[81] The two ways courts can determine Fourth Amendment applicability—physical trespass and reasonable expectation of privacy—were devised due to the need for the law to conform with advances in technology.[82] Whereas one resulted from the progression of physical technology, namely wiretapping, the other was the product of remote, electronic technology.[83] Even after the two methods of determining Fourth Amendment applicability were established, courts continued to hear new cases regarding technology and how it interacted with the Constitution.[84] As such, the law will naturally continue to follow this

77. *White*, 401 U.S. at 752; *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. at 465.
78. *See infra* notes 79–80 and accompanying text.
79. *E.g.*, United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016) (holding that the defendant voluntarily shared his IP addresses with Microsoft, so he had no reasonable expectation of privacy in them); United States v. Christie, 624 F.3d 558, 573–74 (3d Cir. 2010) (holding that because defendant shared his IP address with the websites he visited, the government did not need a warrant to obtain that address through the administrator of one of those websites); United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (holding that defendant had "no Fourth Amendment privacy expectation" in his IP address, which he had shared with Yahoo! by using an online chat service).
80. United States v. Beckett, 369 F. App'x 52, 56 (11th Cir. 2010) (holding that the defendant did not have a reasonable expectation of privacy in his IP address because that information is "transmitted during internet usage" and "is necessary for the . . . [Internet Service Providers] . . . to perform their services"); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that defendant had no reasonable expectation of privacy in the IP addresses of websites he visited because he voluntarily shared that information with his Internet Service Provider, as was necessary to view the websites).
81. *See supra* notes 45–80 and accompanying text.
82. *See supra* notes 45–57 and accompanying text.
83. Olmstead v. United States, 277 U.S. 438, 456–57 (1928); Katz v. United States, 389 U.S. 347, 348 (1967).
84. *See supra* notes 58–80 and accompanying text.

pattern as technology continues to become even more advanced and prevalent in our society. Thus, there is a need for courts to recognize when technology has surpassed the current limits of constitutional case law, rather than merely falling back on precedent pertaining to preexisting technology.

IV. THE FOURTH AMENDMENT CONFUSION BEHIND THE TOR NETWORK

In the aftermath of the FBI's raid on Playpen, the charged defendants began to challenge their charges on the grounds of their Fourth Amendment rights being violated.[85] These defendants motioned to suppress any evidence obtained as a result of the warrant as "fruit of the poisonous tree."[86] District courts around the nation were forced to analyze whether the NIT warrant was constitutionally sound.[87] When analyzing a motion to suppress evidence allegedly obtained in violation of the Fourth Amendment, courts must first determine "whether or not a Fourth Amendment 'search' has occurred."[88] Thus, the district courts generally analyze whether one has a reasonable expectation in one's IP address.[89]

A. *Reasonable Expectation in One's IP Address*

The United States District Court for the Eastern District of Virginia, hearing the case of *United States v. Matish*, first looked toward preexisting case law.[90] It noted that the Ninth Circuit case of *United States v. Forrester* held that a reasonable expectation of privacy cannot exist in one's IP address because Internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[91] However, the court recognized a distinguishing feature that set *Matish* apart from *Forrester*.[92] Unlike Forrester, Matish masked his IP address through the use of the Tor network.[93] Rather than supplying his ISP with information that his IP address had connected to Playpen, Matish effectively informed his ISP that he had connected to a randomly-selected node computer

85. *See* cases cited *supra* note 10.
86. *See* cases cited *supra* note 10.
87. *See* cases cited *supra* note 10.
88. Kyllo v. United States, 533 U.S. 27, 31 (2001).
89. *See* cases cited *supra* note 10.
90. 193 F. Supp. 3d 585, 613–16 (E.D. Va. 2016).
91. *Id.* at 615 (citing United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).
92. *See id.*
93. *Id.*

elsewhere in the world.[94] After glossing over this distinction, the court then turned to the case of *United States v. Farrell*, in which the administrator of Silk Road 2.0—a hidden service notorious for illegal drug sales—was brought to justice.[95] In *Farrell*, the Western District of Washington found that no reasonable expectation of privacy existed in IP addresses hidden via the Tor network.[96] The *Farrell* court noted that "in order for . . . prospective user[s] to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations."[97]

The *Matish* court noted that while "Tor markets itself as a tool to prevent[] people from learning your location," it also warns visitors "that the Tor network has vulnerabilities and that users might not remain anonymous."[98] The court saw Tor's disclaimer as enough to "destroy[] any expectation of privacy in a Tor user's IP address."[99] Accordingly, based on the holding of *Farrell*, Tor's disclaimer, and the opinions of other district courts on this matter, the court held that any expectation of privacy was merely subjective and in no way objectively reasonable.[100]

---

94. *See id.* at 593–94, 615–17.

95. *Id.* at 615–16 (citing United States v. Farrell, No. CR15-029RAJ, 2016 WL 705197, at *1 (W.D. Wash. Feb. 23, 2016)). Silk Road 2.0 was the successor of Silk Road, which was founded by Ross Ulbricht (referred to in the community by his pseudonym of "Dread Pirate Roberts"). Alois Afilipoaie & Patrick Shortis, *Silk Road: After Being Closed Twice, Can the Brand Ever 'Rise Again?,'* SWANSEA UNIV. 1–2 (Jan. 2015), https://www.swansea.ac.uk/media/GDPO%20SA%20silk%20rd%20rise%20again.pdf. After Ulbricht was arrested and Silk Road was seized by the FBI in October 2013, several of its administrators created Silk Road 2.0. *Id.* at 2–3. Silk Road 2.0 and twenty-six other "hidden services" were seized in November 2014 as part of an international law enforcement operation dubbed "Operation Onymous." *Id.*; Julia Buxton & Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, SWANSEA UNIV. 15 (Jan. 2015), http://www.drugsandalcohol.ie/23274/1/Darknet%20Markets.pdf. Brian Farrell was subsequently arrested as an alleged administrator of Silk Road 2.0 after his IP address was identified by the Software Engineering Institute of Carnegie Mellon University, which was conducting research on the Tor network. *Farrell*, 2016 WL 705197, at *1. Within hours of the site's seizure, a Silk Road 3.0 was created and remains in "business" to this day. Afilipoaie & Shortis, *supra*, at 4. Each iteration of Silk Road has operated exclusively on the Tor network. *See id.* at 1.

96. *Farrell*, 2016 WL 705197, at *2.

97. *Id.*

98. *Matish*, 193 F. Supp. 3d at 615–16 (citations omitted) (internal quotation marks omitted).

99. *Id.* at 617.

100. *Id.* at 615–17.

However, the *Matish* court discovered a discrepancy between the current fact pattern and the one presented in *Farrell*.[101] It noted that "the NIT used in this case poses questions unique from the conduct at issue in *Farrell*."[102] In *Farrell*, the government played no role in uncovering the user's IP address.[103] Instead, Farrell's IP address was given to the government by researchers who were operating a node that he connected to.[104] In contrast, the FBI obtained Matish's IP address by sending the NIT code directly into his computer and prompting it to send the desired information to the FBI's computer.[105] Despite this major difference, the court made a finding similar to other district courts, which suggested that knowingly connecting one's IP address to a third party serving as a Tor node is enough to topple any subjective expectation of privacy.[106] Thus, the court held that "any such subjective expectation of privacy—if one even existed in this case—is not objectively reasonable."[107]

This determination—this dismissal of a key fact—defies logic. By the reasoning of the *Matish* court, no communication to any other person would warrant a subjective—much less a reasonably objective—expectation of privacy.[108] Even if one were to privately pass another person a note in an empty, locked room, as long as there exists the possibility of that person revealing the contents of that note, the government would be justified in breaking into the room and reading its contents.

To go even further—in terms of this metaphor—the *Matish* court would likely suggest that the individual even lacks any expectation of privacy to the locked room itself. Indeed, the court proclaimed that

101. *Id.* at 617.

102. *Id.* (emphasis added).

103. *Id.*; *see also* United States v. Farrell, No. CR 15-029RAJ, 2016 WL 705197, at *1 (noting that Farrell's IP address was identified by the Software Engineering Institute of Carnegie Mellon University during the course of its research on the Tor network).

104. *Farrell*, 2016 WL 705197, at *1.

105. *Matish*, 193 F. Supp. 3d at 595, 617.

106. *Id.* at 617. The Western District of Arkansas, one of the other district courts, similarly opined that "on its very first hop, the TOR user's true IP address is disclosed to the first node computer in the TOR chain. Thus, the user's true IP address is not a complete secret." United States v. Jean, 207 F. Supp. 3d 920, 933 (W.D. Ark. 2016). This court further stated that a Tor user takes risks in revealing his IP address to both his Internet Service Provider and the owner of the first node computer in the Tor chain, as either one could provide information to the government. *Id.* Under this reasoning, the Arkansas district court found no reasonable expectation of privacy as to the defendant's IP address, thus no Fourth Amendment implication and no requirement for the FBI to procure a valid warrant. *Id.*

107. *Matish*, 193 F. Supp. 3d at 616.

108. *See id.*

individuals do not even have a reasonable expectation of privacy within their own computers.[109] Despite noting that "[t]he Ninth Circuit found in 2007 that connecting to a network did not eliminate the reasonable expectation of privacy in one's computer,"[110] the court claimed that "hacking is much more prevalent now than it was even nine years ago, and the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy."[111] While the court tried to emphasize this point with numerous articles concerning hacking, it failed to realize the irony in the fact that a majority of the articles discuss major businesses, governments, and other high-profile targets—not private individuals.[112]

While the average individual might not have as much security against hacking as a business or government might, common sense dictates that an experienced hacker would have little to no interest in the contents of the average citizen's computer. As for run-of-the-mill viruses and malware, most can be avoided with diligence and antivirus software.[113] A minimal amount of precaution can keep the average person from exposing his computer to hacking, just like the precaution of using Tor managed to keep many IP addresses from being discovered by the FBI, causing the agency to resort to the use of NIT malware.[114] However, the *Matish* court neglected to consider such precautions, and instead stated that, "in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked."[115]

The *Matish* court likens hacking to an officer taking advantage of a set of broken blinds so that he can peer into one's home.[116] To the contrary, the use of NIT (or any other form of hacking) appears to

109. *See id.* at 615–16.

110. *Id.* at 618 (citing United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007)).

111. *Id.* at 619.

112. *Id.* (citing instances of hacking which targeted Apple, politicians, Ashley Madison, Sony, Home Depot, Target, the *New York Times*, a law firm specializing in intellectual property, and the United States government).

113. *What Are Some Tips for Avoiding Computer Viruses?*, UAB INFO. TECH., https://www.uab.edu/it/home/it-reports-and-publications/item/229-what-are-some-tips-for-avoiding-computer-viruses (last modified Oct. 18, 2012).

114. *Matish*, 193 F. Supp. 3d at 594–95.

115. *Id.* at 619.

116. *Id.* at 620 (citing Minnesota v. Carter, 525 U.S. 83, 85 (1998)). It is important to note that the Supreme Court in *Carter* never reached the issue of whether peering through broken blinds constituted a "search." *Carter*, 525 U.S. at 91. Instead, it was Justice Breyer who stated in his concurring opinion that he believed such conduct did not violate anyone's Fourth Amendment rights. *Id.* at 103 (Breyer, J., concurring).

more closely resemble an officer using the vulnerability of a thin, glass window to shatter it, reach inside, and raise the blinds himself. The FBI could not merely take a closer look to peer inside of a Tor user's computer and subsequently identify his IP address; it had to actively exploit the weaknesses of the Tor network and the user's computer and force the computer to send over the desired information.[117]

In short, *Matish* missed the big picture. A person should not lose a reasonable expectation of privacy in his computer simply because he connects to the Internet. The court was on the right track when it cited 2007 case law that says exactly that, but it quickly veered off course when it claimed that hacking is more prevalent today, with only high-profile targets as its examples.[118] While *Matish* rejects any such notion in the affirmative,[119] it begs the question of whether the use of Tor or other tools to ensure security and anonymity would raise one's subjective expectation of privacy to the level of objective reasonableness.

B. *Reasonable Expectation of Privacy in One's Computer*

In the Western District of Texas, the district court hearing the case of *United States v. Torres* answered the questions of reasonable expectation of privacy in a more simplistic manner.[120] Rather than struggling with the separate questions of whether an expectation of privacy existed in either Torres's computer or IP address, and with case law in these issues being rather scarce, the court thought outside the box.[121] The *Torres* court relied on the 2014 Supreme Court case of *Riley v. California*, which found that "individuals have a reasonable expectation of privacy in their cell phones, due to the extensive amount of personal information contained therein."[122] Presumably, due to the fact that modern-day cell phones are essentially miniature, handheld computers, the *Torres* court determined that "it is reasonable to find that persons also have a reasonable expectation of privacy in their personal computers, due to the vast amount of personal information they contain."[123] While the court kept its explanation on this point rather brief,[124] it could be

117. *Matish*, 193 F. Supp. 3d at 595.
118. *Id.* at 617–19.
119. *Id.* at 620.
120. No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016).
121. *See id.*
122. *Id.* (citing Riley v. California, 134 S. Ct. 2473 (2014)).
123. *Id.*
124. *See id.*

understood that the court suggested that both computers and the information within (i.e. IP addresses) are of such personal importance, that an individual would naturally have a reasonable expectation of privacy in both.

Conversely, whilst rejecting the assertion by many of the other district courts that a person lacks a reasonable expectation of privacy in his IP address alone, the court seemed to suggest that the FBI's conduct was so flagrant in its aim that it need apply neither the physical trespass theory nor the *Katz* test.[125] Instead, the court explained:

> [T]he NIT placed code on Mr. Torres' computer without his permission, causing it to transmit his IP address and other identifying data to the government. That Mr. Torres did not have a reasonable expectation of privacy in his IP address is of no import. This was *unquestionably* a "search" for Fourth Amendment purposes.[126]

Other district courts have reached similar conclusions on this matter.[127] In Florida, the district court addressing the case of *United States v. Adams* cautioned against viewing the issue under the narrow scope of whether a reasonable expectation of privacy exists in a Tor user's IP address and instructed that the proper subject of the analysis is the defendant's computer.[128] The *Adams* court found that a Fourth Amendment search occurred because "Defendant's IP address was discovered only after property residing within Defendant's home—his computer—was searched by the NIT."[129] The court also described its legal reasoning in the form of an analogy:

> [A] defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the "open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of

125. *See id.*
126. *Id.* (emphasis added).
127. *See infra* notes 128–31 and accompanying text.
128. No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016) (stating that although there was no reasonable expectation of privacy in defendant's IP address, the proper subject of the analysis should be the computer).
129. *Id.*

> Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device.[130]

A Massachusetts district court in the case of *United States v. Anzalone* relied on the reasoning in *Adams*, and further noted that

> [w]hile the most critical piece of information obtained by the NIT warrant may have been the IP address, the NIT afforded the government access to six other pieces of identifying information that were not readily available to law enforcement, as well as the ability to pair a user's actions on Playpen with the user's IP address.[131]

Despite such compelling reasoning, some might be inclined to disagree with the simplistic suggestion that a reasonable expectation of privacy in one's computer is sufficient on its own to establish the existence of a Fourth Amendment search.[132] The Fourth Circuit has held that "the appropriate [Fourth Amendment] inquiry . . . [is] whether the individual had a reasonable expectation of privacy in the area searched, not merely in the items found."[133] While this suggests that the *Torres* court's analysis of reasonable expectation of privacy in one's computer is proper, it also stands to reason that the inverse is also true: analyzing one's expectation of privacy in only the area itself—in this instance, the computer—while ignoring whether any expectation of privacy exists in the items found, would not be appropriate, particularly when such items are willingly presented to others over a network.

The *Torres* opinion, while taking a completely different approach, is similar to *Matish* in the sense that both circumvent the issue of whether taking steps to conceal one's IP address—to the extent that not even the FBI can discover it (unless reported by the operator of a node computer or retrieved by invasive means such as the NIT)—could cause an individual's subjective expectation of privacy in his IP address to become objectively reasonable in the eyes of society.[134]

---

130. *Id.* (citation omitted).

131. 208 F. Supp. 3d 358, 366 (D. Mass. 2016).

132. *See, e.g.*, United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986) (noting that an individual must have a reasonable expectation of privacy in the area searched, not just in the items found).

133. *Id.* (citing Rawlings v. Kentucky, 448 U.S. 98, 104–06 (1980)).

134. *Compare* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016) (holding that Torres had a reasonable expectation of privacy in his computer, but neglecting to address whether concealing an IP address was objectively reasonable), *with* United States v. Matish, 193 F. Supp. 3d 585, 616–

V. SOLUTION

Surely, there are an abundance of superb arguments regarding whether the use of the NIT constitutes a Fourth Amendment search—even beyond those described above. Generally speaking, analyzing solely the IP address under the *Katz* test results in a finding of no Fourth Amendment search,[135] whereas a *Katz* analysis of one's personal computer typically gives the opposite result.[136] With such limited authority on the matter, all of which can be easily distinguished by the present key factor of Tor's IP-shielding function, it is no wonder why the courts across the nation are at odds with one another on how to resolve the constitutional issues surrounding the competing technologies of the NIT and Tor.[137]

While the analyses conducted by the various courts tend to revolve around whether there exists a reasonable expectation of privacy in either the user's IP address or computer,[138] both methods of applying the *Katz* test, without more, are flawed. While case law might suggest that the area searched—in this instance, the computers—is the proper subject of the analysis,[139] it is still important to note that a Tor user's IP address is still volunteered to the user's ISP and the owner of the node computer it connects to.[140] Therefore, regardless of whether the area searched requires a *Katz* analysis, the IP address still requires the same analysis, as it is being volunteered to third parties for limited purposes.[141]

A. *Putting Tor's Privacy Feature to the (Katz) Test*

Although many of the district courts analyzed whether the defendants had a reasonable expectation of privacy to their IP addresses, most relied on existing case law that suggested that IP addresses are not subject to a reasonable expectation of privacy because they are openly shared with third parties when they connect

17 (E.D. Va. 2016) (holding that Matish's expectation of privacy in his IP address was not reasonable, but neglecting to consider whether concealing an IP address could be objectively reasonable).

135. *See supra* Section IV.A.
136. *See supra* Section IV.B.
137. *See supra* Part IV.
138. *See supra* Part IV.
139. *See, e.g.*, United States v. Anzalone, 208 F. Supp. 3d 358, 366 (D. Mass. 2016); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016).
140. *See supra* notes 26–27, 73–80 and accompanying text.
141. *See supra* notes 50–57, 62–63 and accompanying text.

to the Internet.[142] However, this generalization is improper. Rather than sharing the IP address, and, by extension, the information of what sites its owner is visiting on the web, with ISPs and the owner of every site visited, the function of Tor limits the IP address's exposure to two parties: the user's ISP and the owner of the first node computer.[143] Furthermore, neither the ISP nor the owner of the first node computer would know the target destination of the Tor user, especially in the event that several nodes are used along the way.[144] Conversely, the owner of the site being connected to does not know the actual IP address of the person visiting it.[145] It is for precisely this reason that the FBI was unable to retrieve the IP addresses of Playpen members without having to place the NIT malware on their computers through the Playpen site itself.[146] It is no stretch to say that Tor's function completely alters the way IP addresses interact on the Internet, which results in a tangled web of privacy.[147] As such, it is improper to subject an IP address under these circumstances to the same reasoning—such as the analysis of *Forrester*—used to analyze a default IP address under *Katz*.

Instead, the proper inquiry should be whether an individual has a reasonable expectation of privacy in his IP address while obscuring it through the use of Tor. While *Matish* conducted an analysis to this effect, the court reached its conclusion that no reasonable expectation of privacy could possibly exist through the premise of hacking

142. *See supra* Section IV.A.

143. *See supra* notes 26–27 and accompanying text. Traditionally, without the use of Tor, one browsing the Internet would be openly sharing his IP address, his general geographical location, and the information regarding what site he is connecting to with numerous parties including his own Internet Service Provider, the owner of each site he visits, the Internet Service Providers that host each site visited, and even other third parties, such as those responsible for online advertisements. *See* Fisher, *supra* note 26.

144. *See* Owsley, *supra* note 36, at 341. The exception to this statement is the scenario that occurred in *Farrell*, where researchers, rather than the government, discovered the IP address. *See* United States v. Farrell, No. CR15-029RAJ, 2016 WL 705197, at *1. While the *Farrell* opinion is similar to those arising from the NIT situation in the sense that it is a ruling merely on a pretrial motion, it is unlike them in the sense that it is a rather brief opinion with scarce details as to how the events unfolded. Authorities were given Farrell's IP address by the owners of the node he connected to: a university-based research program being funded by the Department of Defense. *Id.* It is unclear how the node's owner discovered Farrell's destination, although it seems highly likely that it similarly implemented the use of a "Trojan horse device" as described previously. *See supra* note 36 and accompanying text.

145. Owsley, *supra* note 36, at 341.

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

147. *See id.* at 593–95.

becoming more prevalent in today's society.[148] As previously discussed, such a premise is flawed, as it fails to account for precautions the average person can take when browsing the Internet and would suggest that a search of one's locked suitcase would be permissible merely because the lock could be easily broken.[149]

Similarly, the argument that a third party—namely the owner of the connected node—could possibly disclose the IP address to the authorities is equally flawed.[150] While the owner of the node is indeed a stranger—thus making it unreasonable that one would expect any degree of confidentiality—it is almost equally unlikely that the individual would know the Tor user's destination without the use of tools similar to that of the NIT in order to track all subsequent node connections.[151] Courts must take caution in declaring that the mere possibility that a third party could disclose the information, regardless of whether they had knowledge of any illicit activities, is enough to destroy a potential reasonable expectation of privacy. Such reasoning could just as easily be applied in finding no Fourth Amendment search in the interception of text messages, emails, and phone calls.

Relying on either of the above rationales creates a slippery slope that could strip away the Fourth Amendment rights from citizens merely because an intrusion or unintended disclosure is *possible*, rather than probable. Courts, in determining the reasonableness in one's subjective expectations, should instead question the *probability* of such occurrences. Where a high probability of intrusion or disclosure exists, an expectation of privacy is more likely to be unreasonable.[152]

1. The Subjective Prong

The first step of a *Katz* analysis is to determine whether the individual has a subjective expectation of privacy.[153] While *Matish* makes a valid point regarding Tor's own disclaimer that the Tor network may have "vulnerabilities" that may not always keep the

148. *Id.* at 615–17, 619–20.
149. *See supra* notes 113–15 and accompanying text.
150. *See supra* note 106 and accompanying text.
151. *See supra* notes 116–17 and accompanying text.
152. This should not be read to mean that a high probability will *always* result in unreasonableness. A car parked in a high-crime neighborhood containing an expensive stereo in plain view has a good probability of being broken into. However, this fact alone would not justify police in forcing entry to the vehicle.
153. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

user anonymous,[154] it should be viewed as a single factor under the totality of the circumstances. While Tor does provide such a disclaimer, it is not in plain view on its home page.[155] Instead, its home page advertises that "Tor prevents people from learning your location or browsing habits," and includes a statement on "Why Anonymity Matters," which explains that "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[156] Such an explanation of Tor's functions, despite how rudimentary it may seem, is indeed true, given the fact that not even the FBI could track down its users' identities through traditional, noninvasive means.[157]

The privacy feature that Tor offers is its main purpose.[158] The fact that illicit "hidden services" use Tor is no mere coincidence, but rather a testament to its technological prowess.[159] Between the claims Tor itself makes, the factual description of how it works, and the fact that it is well-renowned—or perhaps notorious—for its capabilities, it is clear how one could easily hold a subjective expectation of privacy in his IP address while it is being concealed by Tor.

2. The Objective Prong

The second, final, and most challenging step of the *Katz* test is to establish that the individual's expectation of privacy is objectively reasonable.[160] This half of the *Katz* test, in this context, asks whether our society would accept an individual's expectation of privacy in his IP while obscured by the Tor network as reasonable.[161]

We live in a society that has been consistently employing technology for security purposes. Over the decades, we have seen the rise of surveillance cameras, metal detectors, digital passwords on

154. United States v. Matish, 193 F. Supp. 3d 585, 616 (E.D. Va. 2016).
155. *See* TOR, https://www.torproject.org/ (last visited Apr. 20, 2018).
156. *Id.*
157. *Matish*, 193 F. Supp. 3d at 593–95.
158. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Apr. 20, 2018).
159. *See* Andy Greenberg, *It's About to Get Even Easier to Hide on the Dark Web*, WIRED (Jan. 20, 2017, 7:00 AM), https://www.wired.com/2017/01/get-even-easier-hide-dark-web/.
160. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
161. *See id.*

devices and services, firewalls, antivirus software, and various other security measures used in our daily lives. Not even a century ago, many of our modern-day security measures would have been viewed as something straight out of a science-fiction novel. Yet, the necessity for both convenience and security in our society has led to outstanding technology and technological security measures to match. Surely, a similar thought must have been in mind when the United States Naval Research Laboratory invented the tool now known as "Tor."[162]

The Internet has become an icon of modern-day technology and convenience. As of 2016, over three-fourths of all people in the United States use the Internet.[163] To access the Internet, one typically must connect to it through an ISP.[164] Although this connection may be secure from most other individuals, it is anything but private, as one's IP address and geographical location is disclosed to the ISP and the operator of any website being accessed.[165] Many people who are aware of this fact and are unsatisfied with the lack of full privacy and anonymity have turned to services such as Tor to add an extra layer of protection and privacy.[166] Although Tor users must still connect their IP address to a node computer, the amount of disclosure through Tor is minimal, especially in comparison to Internet use without it.[167]

It is imperative to note that Tor is not some niche software that is only used by a handful of people. In 2010 alone, Tor was downloaded over thirty-six million times.[168] Several institutions, recognizing Tor's potential for security, have provided grants to the Tor Project, including Google, Human Rights Watch, and even the

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

163. *See Individuals Using the Internet (% of Population)*, WORLD BANK, https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2016&start=1960&view=chart (last visited Apr. 20, 2018) (showing that the total percentage of the United States population using the Internet in 2016 reached 76 percent).

164. Tim Fisher, *Internet Service Provider (ISP)*, LIFEWIRE, https://www.lifewire.com/internet-service-provider-isp-2625924 (last updated Apr. 11, 2018).

165. *See id.*; *see also* Cale Guthrie Weissman, *What Is an IP Address and What Can It Reveal About You?*, BUS. INSIDER (May 18, 2015, 4:45 PM), http://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5 (explaining that geo-location is shared in an IP address).

166. *See, e.g.*, Nathaniel Rich, *The American Wikileaks Hacker*, ROLLING STONE (Dec. 1, 2010), https://www.rollingstone.com/culture/news/meet-the-american-hacker-behind-wikileaks-20101201 (noting that Jacob Appelbaum, an American member of Wikileaks, uses Tor in the Wikileaks operation).

167. *See id.*

168. *Id.*

United States military.[169] Additionally, activist groups such as the Electronic Frontier Foundation have praised Tor's capabilities and recommend it "as a mechanism for maintaining civil liberties online."[170] Even the International Broadcasting Bureau, part of the Broadcasting Board of Governors—an independent United States agency—supports Tor development for countries where safe access to free media is restricted or unlawful.[171]

Countless people and institutions have taken note of the security and anonymity the Tor network can provide.[172] The Tor Project itself publicly provides an in-depth, technical explanation, complete with diagrams, of how the network functions and provides more security to its users compared to those who connect to websites directly.[173] For these reasons, our society—one that values security, privacy, and safety (and often utilizes technology to achieve it)—would most certainly be willing to find that an individual's perceived expectation of privacy in his IP address is perfectly reasonable when it is shielded by world-renown, technologically-sound software.

The public information available on the history of Tor and how it functions more than supports a subjective expectation of privacy in one's IP address when it is masked by the Tor network.[174] Likewise, the aforementioned information, combined with the public's acceptance of Tor's capabilities supports a finding that there is an objectively reasonable expectation of privacy as well.[175] Thus, both prongs of the *Katz* test would be satisfied, which indicates that the use of the NIT or other means to invade a Tor user's computer and retrieve his IP address constitutes a Fourth Amendment search; accordingly, to take actions in obtaining one's hidden IP address or other concealed information would first require a valid warrant.[176] Therefore, *Matish* and like-minded courts are incorrect in declaring

169. *Id.*

170. *Tor: Overview*, *supra* note 158.

171. *See Tor: Sponsors*, TOR, https://www.torproject.org/about/sponsors.html.en (last visited Apr. 20, 2018) (listing current and former sponsors); *see also Who Uses Tor?*, TOR, https://www.torproject.org/about/torusers.html.en (last visited Apr. 20, 2018) (explaining that individuals living "behind national firewalls or under the surveillance of repressive regimes" use Tor).

172. *See Who Uses Tor?*, *supra* note 171.

173. *Tor: Overview*, *supra* note 158.

174. *See id.*; *see also Who Uses Tor?*, *supra* note 171 (describing how users expect Tor to help protect and maintain their privacy while using the Internet).

175. *See supra* notes 163–74 and accompanying text.

176. *See supra* notes 50–55, 68, 174–75 and accompanying text.

that no warrant is necessary for a search under these circumstances.[177]

B. *Statutory Implications*

Changes to the Federal Rules of Criminal Procedure (FRCrP) in 2016 also suggest that a valid warrant is required to overcome the obstacles Tor causes for the administration of justice.[178] Throughout that year, there was much disagreement between the various district courts over the constitutionality of the NIT searches and whether the NIT warrant issued in the Eastern District of Virginia was valid outside of the jurisdiction under Rule 41 of the FRCrP.[179] Congress, presumably taking note of the judicial incongruity, amended Rule 41, and the changes became effective on December 1, 2016.[180] The amendment brought the adoption of FRCrP 41(b)(6)(A), which reads:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means.[181]

Although this new text does not expressly refer to IP addresses and the use of Tor or similar software, it is heavily implied by the timing and the circumstances surrounding this amendment that this scenario is exactly what Rule 41(b)(6)(A) is aimed at resolving.[182]

---

177. *See supra* notes 79–80, 108, 153–76 and accompanying text.

178. *See* Susan Hennessey, *Rule 41: Resolving Procedural Debates to Face the Tough Questions on Government Hacking*, LAWFARE (Dec. 1, 2016, 2:38 PM), https://www.lawfareblog.com/rule-41-resolving-procedural-debates-face-tough-questions-government-hacking#.

179. *Id.*

180. *See id.* Prior to the amendment, the rule laid out various scenarios in which a magistrate judge was permitted to issue a warrant, including exceptions to the general rule that a magistrate could not issue a warrant outside of his own jurisdiction. *See* FED. R. CRIM. P. 41(b)(1)–(5) (2014) (amended 2016). However, none of the exceptions appeared to exempt the use of the NIT and similar tools from the general rule. *See id.*

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

182. *See* Hennessey, *supra* note 178 ("The amendment is designed to authorize the issuance of precisely the kind of search warrant the FBI obtained in the Playpen operation.").

This new exception means a lot more than merely allowing magistrate judges to issue warrants in scenarios such as those seen in the Playpen FBI operation. The fact that Congress added this language in an amendment means that the use of NIT or similar tools to bypass software such as Tor is in fact a search under the Fourth Amendment, thus requiring a valid warrant. While there is nothing in the rule that expressly demands a warrant be issued to utilize such tools, it seems apparent, by its granting of authority to grant such warrants, that a warrant is necessary.

After all the disagreement and confusion between district courts,[183] Congress seems to have quelled their bickering and resolved this issue.[184] Should any courts continue to struggle with the issue of whether or not a warrant is mandated for the use of the NIT or any other "Trojan horse device" in the government's arsenal, it may come down to federal courts to interpret FRCrP 41(b)(6)(A). However, at least for now, the amendment appears to be the answer to this situation, regardless of whether the courts agree with its implications.

VI. CONCLUSION

Time and time again, our judicial history has shown a need for the law to adapt to our evolving society and its many technological advancements.[185] In 2016, district courts across the nation struggled with yet another instance of the law lagging behind technology.[186] When individuals found ways to further complicate the functions of IP addresses to enhance their privacy, law enforcement was required to develop and utilize tools to uncover the identities and locations of criminals using technology to remain anonymous.[187] Whereas the law at the time authorized the issuing of warrants for law enforcement to utilize technology in a variety of ways, the use of the NIT to uncover an anonymous user was not one of them.[188] When it was revealed that the law did not account for the use of either technology, courts were left to argue whether a warrant was even

183. *Id.* (discussing the fact that prior to the amendment, federal district court judges had "diverged significantly in their analyses and conclusions" regarding cases relating to the issue of "whether the warrant for a network investigative technique designed to obtain the IP address of computers accessing contraband child sexual abuse materials, authorized in the Eastern District of Virginia, violated Rule 41 when applied to computers outside that district").

184. *Id.*

185. *See supra* Part III.

186. *See supra* Parts II, IV.

187. *See supra* Part II.

188. FED. R. CRIM. P. 41(b)(1)–(5) (2014) (amended 2016).

required for such a purpose.[189] However, it appears as though the law has once again caught up with society, with the amendment to FRCrP 41.[190]

All in all, this is yet another prime example of the law's inability to keep up with our society's technological developments, and the necessity for it to do so. As a result, countless hours and dollars were spent on litigation across the nation, and much frustration ensued. Yet, as the saying goes: "History tends to repeat itself." It is only a matter of time before this digital age of ours tests the limits of the law once more.

189. *See supra* Part IV.

190. *See supra* Section V.B.