IS A SINGLE CLICK OF A URL ENOUGH FOR A SEARCH WARRANT?: A LOOK AT THE EXPANSION OF PROBABLE CAUSE IN CHILD PORNOGRAPHY INVESTIGATIONS

Sydney Hope*

I. INTRODUCTION AND PROBABLE CAUSE

The right to privacy is a fundamental right guaranteed by the United States Constitution.[1] However, as the Internet and technology have evolved a natural tension between the right to privacy and the investigation of cybercrimes emerged.[2] There must be a line between these seemingly contradictory interests and there is a history of court cases attempting to find where the line is between an individual's privacy and the methods law enforcement can use to find perpetrators of crimes.[3] While this Note focuses specifically on recent cases involving the possession of child pornography, the issues presented are widespread and affect the right to privacy of every person who uses the Internet.[4]

The Fourth Amendment of the United States Constitution assures the "right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"

* Sydney Hope is a candidate for Juris Doctor at SMU Dedman School of Law. She graduated from the University of Texas at Austin with a Bachelor of Science in Communication Studies in 2017.

1. Paul Larkin Jr., *The Fourth Amendment and New Technologies*, THE HERITAGE FOUNDATION (Sept. 13, 2013), https://www.heritage.org/report/the-fourth-amendment-and-new-technologies.

2. Erin Larson, *Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?*, 18 N.C. J.L. & TECH. 316, 321 (2017).

3. *See id.*

4. Aaron Mackey, *A Click on a URL Isn't Enough for a Search Warrant*, ELECTRONIC FRONTIER FOUNDATION (Aug. 31, 2018)), https://www.eff.org/press/releases/click-url-isnt-enough-search-warrant.

without a warrant.[5] Under this Amendment, a warrant cannot be issued unless there is probable cause for the search.[6] In determining probable cause, the judge only needs to make a "practical, common-sense decision whether given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."[7] The probability that evidence will be found in the place to be searched does not have to be certain, so long as the judge has a rational basis for his or her belief.[8]

However, as technology has evolved it has become easier to track the online activity of individuals through their IP address.[9] Law enforcement agencies frequently use this information as evidence to establish probable cause for a search warrant.[10] The practice of using software to track IP addresses of individuals is routinely used when investigating possession of child pornography.[11] Some circuit courts have found an IP address connected with such activity was enough to establish probable cause to search the individual's residence.[12] The Second Circuit, on

5. U.S. CONST. amend. IV.

6. *Id.*

7. Illinois v. Gates, 462 U.S. 213, 238 (1983).

8. *Id.* at 236.

9. Larson *supra* note 2, at 322.

10. *Id.* at 326.

11. Zoe Russel*, First They Came for the Child Pornographers: The FBI's International Search Warrant to Hack the Dark Web*, 49 ST. MARY'S L.J. 269, 270 (2017).

12. United States v. Contreras, 905 F.3d 853, 858 (5th Cir. 2018); United States. v. Richardson, 607 F.3d 357, 370–71 (4th Cir. 2010); United States. v. Vosburgh, 602 F.3d 512, 527 (3d Cir. 2010).

the other hand, found that there was no probable cause to search an individual's residence or computer based only on minimal online activity.[13]

In the recent case *United States v. Boysk*, the Fourth Circuit followed the reasoning of the circuits finding probable cause based on an individual's IP address being linked with a URL that contained child pornography.[14] However, the court in this case went further than existing cases by finding that a single click of a URL held on a file sharing website was sufficient evidence to establish probable cause to search the defendant's home.[15] Thus, the court set a precedent for a reduced standard of probable cause that applies not only to cases of possession of child pornography, but also to criminal investigations in a larger context.[16]

Part II of this Note provides an overview of existing case law regarding probable cause and child pornography cases. Part III introduces the recent case *United States v. Bosyk* and the court's reasoning in the case. Part III then analyzes the court's erroneous use of the previous law discussed in Part II to arrive at an incorrect holding. Part IV discusses the implication the court's flawed decision will have on the right to privacy as technology continues to evolve.

II. BACKGROUND OF EXISTING LAW REGARDING CHILD PORNOGRAPHY AND PROBABLE CAUSE

13. United States v. Raymonda, 780 F.3d 105 (2d Cir. 2015); United States v. Falso, 544 F.3d 110, 124 (2d Cir. 2008).

14. United States v. Bosyk, 933 F.3d 319, 325–26 (4th Cir. 2019).

15. *Compare id.* at 334 (holding that there was probable cause based on a single click of a URL), *with Richardson*, 607 F.3d at 370–71 (holding there was probable cause because the defendant used an AOL account to send images), *and Vosburgh*, 602 F.3d at 517 (finding there was probable cause because "a user seeking to access a link to child pornography posted on Ranchi cannot do so with the simple click of the mouse")).

16. *See Bosyk*, 933 F.3d at 334.

A. Cases Where Probable Cause for Search Warrant Was Established

In previous cases, courts have found sufficient probable cause based on activity more than a click on a URL.[17] For example, in *United States v. Vosburgh*, the Third Circuit found there was probable cause to search the defendant's computer based on his IP address being linked with activity on a child pornography website.[18] A user attempted to download a dummy link posted by an FBI agent on the child pornography website Ranchi.[19] The FBI computer generated a log file containing the IP address of every user who attempted to access the link and the date and time of each attempt.[20] This dummy link started with "hxxp," so the users who accessed the link had to paste it in their address bar and change it to http for the link to be recognized by the browser.[21] The IP address assigned to the defendant was linked to a user who attempted to download the link on the same day it was posted three times in a two-minute period.[22] The affidavit for the search warrant included the time and date that the IP address attempted to access the link, the steps taken by the agent to track the IP address to the defendant's physical address, and the steps taken to confirm the defendant lived at the address.[23] The Third Circuit found that evidence that a user of a computer employing a particular IP address that possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address, even if it did not

17. *See, e.g., Vosburgh*, 602 F.3d at 517.

18. *Id.* at 527.

19. *Id.* at 517–18.

20. *Id.*

21. *Id.* at 517.

22. *Id.* at 517–18.

23. *Vosburgh*, 602 F.3d at 518–19.

conclusively link the pornography to the residence.[24] The "unique nature" of the IP address assigned to the defendant traced the attempts to access the content to his Comcast account and the residence the account was registered to.[25]

In a similar case in the Fourth Circuit, the court held there was probable cause for a search when an AOL email address was reported to be sending emails containing child pornography.[26] In this case, AOL reported to the cyber tip line at the National Center for Missing and Exploited Children (NCMEC) that they had detected the transmission of child pornography images by an email address which was registered to the defendant.[27] A year later, AOL reported another email containing child pornography from a different email address registered to the defendant at another physical address.[28] The investigation revealed the defendant's current physical address and linked him to both addresses connected to the email accounts.[29] Based on the totality of circumstances presented in the affidavit—the information disclosed by AOL as well as details from the investigation conducted by the agent that linked the defendant to the two email addresses—the court found there was sufficient reason to believe that contraband or evidence would be found in the place to be searched.[30]

---

24. *Id.* at 526.

25. *Id.* at 527.

26. United States v. Richardson, 607 F.3d 357, 370–71 (4th Cir. 2010).

27. *Id.* at 360.

28. *Id.* at 361.

29. *Id.*

30. *Id.* at 361, 370–71.

The Fifth Circuit similarly found probable cause when an undercover Homeland Security Investigations officer saw that a user posted explicit images to a group chat on Kik on two different dates.[31] Kik provided the IP address which was registered to the defendant's father and law enforcement confirmed that the family lived at the residential address connected to the account.[32] The court found that there was a fair probability that the user lived in the home and there was precedent for probable cause based solely on a few uploads of child pornography.[33]

There are several other examples of cases that have found probable cause based on the defendant's online activity.[34] An important fact in these cases is that the defendant in every case was a member or subscriber of a website containing child pornography.[35] As illustrated by the cases discussed above, the courts consistently focused on additional evidence outside of clicking a link to establish probable cause.[36] In *Vosburgh*, the link had to be edited by the user before it could be used.[37] And in both *Richardson* and *Contreras*, the defendants were the ones who sent or

31. United States v. Contreras, 905 F.3d 853, 855 (5th Cir. 2018).

32. *Id.* at 856.

33. *Id.* at 858.

34. *See, e.g.,* United States v. Gourde, 440 F.3d 1065, 1071 (9th Cir. 2009).

35. United States v. Falso, 544 F.3d 110, 120 (2d Cir. 2008).

36. *See Contreras,* 905 F.3d at 858 (basing probable cause on uploads of child pornography that was linked to defendant's residence); United States v. Richardson, 607 F.3d 357, 370–71 (4th Cir. 2010) (basing probable cause on the fact that the defendant used an AOL account to send explicit images); United States v. Vosburgh, 602 F.3d 512, 517–18 (3d Cir. 2010) (basing probable cause on the fact that the defendant accessed a dummy link posted by an agent on a child pornography website).

37. *Vosburgh*, 602 F.3d at 517.

uploaded the material.[38] Contrary to the holding in *Bosyk*, these cases establish that merely clicking on a link is not sufficient for probable cause.[39]

B. Second Circuit Approach: No Probable Clause for Search Warrant

Furthering the conclusion that the court in *Bosyk* was incorrect by finding that clicking on a link is sufficient for probable cause, the Second Circuit has held that there was a lack of probable cause for a search warrant without additional online activity.[40] In *United States v. Falso*, the FBI obtained the IP address of a website which posted images of child pornography and advertised additional child pornography that was hidden until a membership was purchased.[41] The examination of the website revealed the email addresses and other information of possible subscribers.[42] One of these email addresses was linked to the defendant.[43] The affidavit also stated the "residential address associated with [the defendant] had active internet service during the period immediately preceding the warrant request."[44] Further, the affidavit stated it "appeared" defendant "either gained access or attempted to gain access to the [non-member] website."[45] The Second Circuit found that the previous cases finding probable cause were not relevant because the

38. *Contreras*, 905 F.3d at 858; *Richardson,* 607 F.3d at 370–71.

39. *See Falso*, 544 F.3d at 114.

40. *See, e.g.*, *Falso*, 544 F.3d at 120.

41. *Id.* at 113–14.

42. *Id.* at 114.

43. *Id.*

44. *Id.*

45. *Id.*

defendant was "not alleged to have actually accessed or subscribed" to the website.[46] While membership or subscription to the site is not required, when the defendant is not a member there needs to be other evidence the defendant otherwise downloaded illegal images.[47] In this case, the court found the affidavit lacked information about whether the images were "prominently displayed or required an additional click of the mouse; whether the images were downloadable; or what other types of services and images were available on the site."[48] Thus, there was not a fair probability that evidence or contraband would be found in the search.[49]

Similarly, the Second Circuit found no probable cause in *United States v. Raymonda*.[50] In this case, an agent obtained a search warrant for a website containing child pornography and got records including IP logs for individual users who had visited the website.[51] These logs indicated the files the users' browser had accessed or attempted to access when the access or attempt occurred.[52] The IP address associated with the defendant accessed seventy-six images, mostly thumbnails, and did not indicate any requests for full-sized images.[53] The court held that a single incident of access did not create a fair probability that illegal material would still be present in the

46. *Falso*, 544 F.3d at 120.

47. *Id.* at 124.

48. *Id.* at 121.

49. *See id.* at 120.

50. United States v. Raymonda, 780 F.3d 105, 117 (2d Cir. 2015).

51. *Id.* at 109.

52. *Id.* at 110.

53. *Id.*

defendant's home.[54] The inference that a defendant was a collector of child pornography, and thus there would still be evidence in the home, was not based on a single click.[55] Rather, it was based on circumstances showing that the defendant had "accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection."[56] These two cases illustrate that, contrary to the holding in *Bosyk*, a simple click of the mouse is not enough to establish probable cause.[57] Rather, as these cases illustrate, there needs to be some additional activity that would lead a reasonable person to believe that evidence or contraband would be present in the defendant's home.[58]

III. UNITED STATES V. BOSYK

A. Facts of the Case

In *Boysk*, the Department of Homeland Security was investigating an online message board which was "dedicated to the advertisement, distribution, and production of child pornography."[59] One day a member of the message board posted a message that described the content of four videos.[60] Below this message there were twenty images depicting child pornography and a URL which contained a random string of numbers and letters.[61] The post also contained a password

54. *Id.* at 117.

55. *Id.* at 115.

56. *Raymonda,* 780 F.3d at 115.

57. *See Raymonda*, 780 F.3d at 117; United States v. Faslo, 544 F.3d 110, 121 (2d Cir. 2008).

58. *Raymonda*, 780 F.3d at 115; *Faslo,* 544 F.3d at 120.

59. United States v. Bosyk, 933 F.3d 319, 322 (4th Cir. 2019).

60. *Id.* at 323.

61. *Id.*

which users needed in order to access the file's content.[62] The link and its contents were held on a filesharing site.[63] The filesharing site produced records showing that on the same day the link was posted to the message board, an IP address "'was used to download or attempt to download file content associated with' the URL containing the four videos" at 3:23 p.m.. [64] However, the affidavit to support probable cause did not indicate what time the link was posted on the message board.[65] Through a subpoena to a broadband provider, investigators were able to connect the IP address to the defendant's house.[66] Also included in the affidavit was a description of "characteristics of individuals who possess or access with intent to view child pornography."[67] These characteristics included keeping the materials for long periods of time and keeping the materials close by.[68]

B. Court's Reasoning

The majority in *Bosyk* focused on the "critical fact" of timing in its reasoning.[69] It heavily relied on the fact that the link was posted on the message board on the same day that it was accessed through the file share site.[70] The court used this fact to piece together assumptions that the link

62. *Id.*

63. *Id.*

64. *Id.*

65. *Bosyk*, 933 F.3d at 326.

66. *Id.* at 323.

67. *Id.*

68. *Id.*

69. *Id.* at 325.

70. *Id.*

was accessed after seeing it on the message board.[71] This would mean it is "fair to conclude" that the user knew it was child pornography because that was the purpose of the message board.[72] Given this assumption, the court further assumed that the same person who clicked on the link typed in the password, downloaded, and viewed the content in the link.[73] The court made this assumption even though there was no evidence presented in the affidavit to support it.[74]

The majority argued the assumption was warranted because it was the "much likelier scenario" based on the facts.[75] The scenario of the defendant innocently coming across the link on the file share site was not enough to defeat probable cause.[76] The court also believed it was unlikely for the material to travel outside of child pornography circles because consumers of this material take extreme measures to conceal their online activities.[77] Further, the court was not persuaded by the fact that the user did not know the link contained child pornography because the URL contained only random letters.[78] However, this is only the case under the majority's "much likelier scenario." Without any additional evidence that the defendant actually accessed the URL through the message

71. *Bosyk*, 933 F.3d at 325.

72. *Id.*

73. *Id.*

74. *Id.* at 365 (Wynn, J., dissenting).

75. *Id.* at 326 (Diaz, J., majority opinion).

76. *Id.*

77. *Bosyk*, 933 F.3d at 327.

78. *Id.* at 328.

board, which there is no evidence of,[79] it is possible that the defendant did not know the content of the link when he clicked on it.[80]

In its discussion of precedent, the court distinguished *United States v. Falso* because the issue in *Falso* was that the affidavit did not allege the defendant actually gained access to a website containing child pornography.[81] The court said the affidavit in *Bosyk* was different because it alleged that the URL contained child pornography.[82] Thus, the inference that the defendant accessed a website containing child pornography, which was missing from *Falso*, was present in this case.[83] However, while the affidavit in *Bosyk* alleged that the defendant accessed the URL, there was no evidence, other than the court's assumptions, that the defendant actually downloaded or viewed the content.[84] The court further differentiated *Bosyk* from other cases that required additional facts "over and above the single click of a URL" because they believed the additional fact of the timing between when the link appeared on the message board and when the defendant accessed it was a sufficient additional fact.[85] However, as discussed above, these cases relied on additional facts showing the defendant actually viewed the material, not merely the timing of when

79. *See id.* at 340–41 (Wynn, J., dissenting).

80. *See id.* at 342 (Wynn, J., dissenting).

81. *Id.* at 329 (Diaz, J., majority opinion).

82. *Id.*

83. *Bosyk*, 933 F.3d at 329.

84. *See id.* at 358 (Wynn, J., dissenting).

85. *Id.* at 330 (Diaz, J. majority opinion).

the URL was clicked on.[86] The court recently affirmed this reasoning by rejecting an appeal to rehear the case en banc.[87]

C. Analysis of the Court's Reasoning

In *Bosyk*, the court incorrectly held that there was probable cause for the search based on the cases above that established probable cause.[88] However, the facts in *Bosyk* differ significantly from the cases the court relied on.[89] The court used *Richardson*, *Vosburgh* and *Contreras* to reason that the magistrate judge's knowledge that someone at the defendant's home clicked on the link was sufficient for probable cause to search the home.[90] The court presumed that the defendant was aware of what the link contained.[91] In each of these cases, the defendant took steps beyond clicking on a link to access the illegal material.[92] However, in *Bosyk*, the defendant was not a member of the website, did not send the material, and did not have to make any changes to the link in order to access the illegal material.[93]

86 . *See* United States v. Raymonda, 780 F.3d 105, 115 (2d Cir. 2015).

87. United States v. Bosyk, 786 F. App'x 398, 398 (4th Cir. 2019).

88. *See Bosyk*, 933 F.3d at 330.

89. *See id.* at 335 (Wynn, J., dissenting).

90. *Id.* at 325–26 (Diaz, J. majority opinion).

91. *Id.* at 325.

92. *See, e.g., Raymonda*, 780 F.3d at 115.

93. *Bosyk*, 933 F.3d. at 335 (Wynn, J., dissenting).

Rather, the facts presented in *Bosyk* are more similar to *Falso* and *Raymonda*.[94] The records in this case only alleged that the defendant downloaded or attempted to download the material on a single date.[95] Since there was no other facts indicating illegal activity, the court incorrectly followed the approach previously followed by other courts; and instead, the Bosyk court should have used the reasoning in *Falso* and *Raymonda* to find there was no probable cause for a search warrant.[96]

The court extended the reasoning of the cases discussed above, finding probable cause in a situation that was not warranted based on the previous case law.[97] In *Bosyk*, the court formed assumptions based on the reasoning in these cases, but did not have sufficient evidence to support the assumptions that it made.[98] Rather, the court made sweeping generalizations that all turned on the single fact of when a URL was accessed.[99] If the court were truly following these other cases, there would have been no probable cause because the fact of timing is not analogous to the substantial evidence produced in the affidavits in each of the previous cases.[100] Given the court's lack of evidence to support the reasoning in *Richardson*, a better approach would have been for

---

94. *Compare id.* at 323 (where an IP address connected with defendant's residence accessed a single link on a filesharing site), *with Raymonda*, 780 F.3d at 110 (where a user accessed thumbnail images a single time in seventeen seconds), *and* United States v. Falso, 544 F.3d 110, 114 (2d Cir. 2008) (where an account associated with the defendant was identified as possible subscriber on a non-member website).

95. *Bosyk*, 933 F.3d at 323.

96. *See id.* at 356–57 (Wynn, J., dissenting).

97 . *See id* at 370.

98. *See id.*

99. *See id.*

100. *See* case cited *supra* note 36.

the court to require more evidence that the defendant collected child pornography, rather than the single instance in this case.[101] If the court applied the factually analogous cases, the court would not have found probable cause.[102] Similarly to these cases, the affidavit in *Bosyk* did not put forth any evidence that the defendant actually viewed or downloaded the content of the URL.[103] The court should have insisted on more evidence of the illegal activity before allowing the home to be searched.[104]

IV. IMPLICATION OF THE *BOSYK* HOLDING

By incorrectly applying its own precedent, as well as the reasoning of other courts, the Fourth Circuit opened the door to violations of the right of privacy for not just those looking at child pornography, but any Internet user.[105] The court said they are sensitive to the privacy interests in the case, but that many serious crimes can be "committed with just a few clicks of a mouse."[106] And under these circumstances, the court must determine whether that information justifies a

101. *Compare Bosyk*, 933 F.3d at 334 (finding probable cause based on a single click on a link containing child pornography), *with Richardson*, 607 F.3d at 370–71 (finding probable cause because the defendant sent several emails containing child pornography).

102. *Compare Bosyk*, 933 F.3d at 334 (finding probable cause based on a single click on a link containing child pornography), *with* United States v. Raymonda, 780 F.3d 105, 115 (2d Cir. 2015) (failing to find probable cause because the court relied on the inference that an individual collected child pornography by "willfully and deliberately, actively seeking" it out rather than a single incident), *and* United States v. Falso, 544 F.3d 110, 121 (2d Cir. 2008) (failing to find probable cause because the affidavit lacked "information about whether the images were prominently displayed or required an additional click of the mouse").

103. *Bosyk*, 933 F.3d at 323.

104. Larson, *supra* note 2, at 335.

105. Mackey, *supra* note 4.

106. *Bosyk*, 933 F.3d at 334.

search of a citizen's home.[107] However, the court did not seriously consider the decision's larger implications for the privacy of other citizens.[108] While the violation of Bosyk's right to privacy may not seem egregious because of the nature of the crime, the court's reasoning can apply to situations beyond these specific facts.[109] Once we allow police to "trample on the privacy rights of individuals suspected of reprehensible crimes, we erode everyone's constitutional rights."[110]

Through this holding, the court drew the line between privacy rights of citizens and the ability of law enforcement to investigate cybercrimes.[111] This line, however, was drawn based on assumptions of the court, not facts.[112] Thus, so long as law enforcement can make general assumptions that a crime was committed based on a single time a user clicked on a URL, that user has effectively opened their home up to a search.[113]

V. CONCLUSION

In *United States v. Bosyk*, the court found probable cause to search the defendant's home simply by the click of a URL.[114] In its reasoning, the Fourth Circuit relied on previous cases—including one decided in its own circuit—that established probable cause for a search based on the

107. *Id.*

108. *See* Mackey, *supra* note 4.

109. *See id.*

110. *Id.*

111. *See* Larson, *supra* note 2, at 321.

112. *See Bosyk*, 933 F.3d at 370 (Wynn, J., dissenting).

113. *See* Mackey, *supra* note 4.

114. *Bosyk*, 933 F.3d at 334.

defendant's online activity.[115] However, these previous cases all rested on more activity than was alleged in *Bosyk*.[116] Further, previous cases found no probable cause based on mere clicks of a URL without more evidence.[117] But, despite the factual similarities between these cases and *Bosyk*, the court did not follow this reasoning.[118] Rather, the court incorrectly applied its own precedent in *United States v. Richardson* and cases from other circuits to erroneously find that probable cause can be established from a single click on a URL.[119]

The court's holding in *Boysk* has serious implications for the privacy rights of every Internet user. With advances in technology, it is easier than ever for investigators to monitor an individual's online activities.[120] Courts do not need to make it even easier for investigators to intrude on an individual's privacy by allowing a simple click of a URL to open the door to a full search of the home. Rather, with increases in technology, even more evidence of illegal activity should be required of investigators to establish the fair probability that evidence or contraband will be found at the home before they are allowed to infringe on a citizen's right to privacy.[121]

115. *Id.* at 325–26.

116. *See* cases cited *supra* note 36.

117. *See, e.g.*, United States v. Falso, 544 F.3d 110, 121 (2d Cir. 2008).

118 . *See Bosyk*, 933 F.3d at 356–57 (Wynn, J., dissenting).

119. *See id.*

120. *See* Larson, *supra* note 2 at 322.

121. *See id.* at 335; *see also* Mackey, *supra* note 4.