NEW YORK LAW SCHOOL

NYLS Law Review
Vols. 22-63 (1976-2019)

Volume 62
Issue 2 *Exploring the Things in the Internet of Things: Implications For Business, Consumers, and the Law*

Article 3

January 2018

United States v. Ammons

Rebecca Ruffer
New York Law School

VOLUME 62 | 2017/18

REBECCA RUFFER

United States v. Ammons

62 N.Y.L. Sch. L. Rev. [•] (2017–2018)

ABOUT THE AUTHOR: Rebecca Ruffer (J.D. candidate, 2018) is the Editor-in-Chief of the 2017–2018 *New York Law School Law Review*.

The internet changed the world. It has transformed the way we learn, interact, and exist.[1] Following each technological innovation advancing society, though, are criminals exploiting that same technology to advance their illegal pursuits.[2]

Today, the internet has become an easily accessible base for people "to create, access, and share child sexual abuse images worldwide at the click of a button."[3] Since 2002, the National Center for Missing and Exploited Children's Child Victim Identification Program[4] has reviewed more than 209 million images and videos and has aided law enforcement in identifying over 13,300 child victims.[5]

In *United States v. Ammons*, the U.S. District Court for the Western District of Kentucky considered whether the FBI's use of a network investigative technique (NIT) without a valid warrant violated the defendant's Fourth Amendment right to be free from unreasonable searches.[6] Even though the defendant, Dennis Ammons, was operating on an underground internet program that obscured his internet protocol (IP) address,[7] the NIT provided the FBI with Ammons' true IP address

---

1. *See generally* James Wei, Great Inventions that Changed the World (2012) (discussing the invention of the internet, its effect on society, and the basis it provided for the development of numerous other inventions).

2. *See, e.g.*, Tom Simonite, *Bitcoin's Dark Side Could Get Darker*, MIT Tech. Rev. (Aug. 13, 2015), https://www.technologyreview.com/s/540151/bitcoins-dark-side-could-get-darker (noting the criminal downside to Bitcoin and exploring the potential "new wave of criminal innovation" stemming from smart contracts); Marc Goodman, *How Technology Makes Us Vulnerable*, CNN, http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/index.html (last updated July 29, 2012, 9:54 AM) (pointing to the role of smartphones, satellite imagery, and night-vision goggles in the 2008 Mumbai terrorist attacks); Matt Wordsworth, *'Stalker Apps' and GPS Allow Domestic Violence Abusers to Discover Hidden Refuges*, ABC, http://www.abc.net.au/news/2015-06-28/stalker-apps-and-gps-endanger-domestic-violence-victims/6570882 (last updated June 27, 2015, 10:59 PM) (profiling the rise of stalkers using tracking technologies to discover hidden victims at refuges).

3. *Child Pornography*, U.S. Dep't Just., https://www.justice.gov/criminal-ceos/child-pornography (last updated June 3, 2015) [https://web.archive.org/web/20170630034829/https://www.justice.gov/criminal-ceos/child-pornography].

4. The Child Victim Identification Program aids in finding and rescuing child victims depicted in sexually exploitive images and videos. *Key Facts*, Nat'l Ctr. for Missing & Exploited Child., http://www.missingkids.org/KeyFacts (last visited Apr. 10, 2018).

5. *Id.*

6. 207 F. Supp. 3d 732 (W.D. Ky. 2016). The Fourth Amendment provides that

> [t]he 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.

U.S. Const. amend. IV.

7. An IP address is a unique numerical label assigned to every machine—a computer or a router, for example—that is part of a network. 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. *See generally* Info. Scis. Inst., Univ. of S. Cal., DOD Standard Internet Protocol (1980), https://tools.ietf.org/pdf/rfc760.pdf (exploring in-depth the IP system as a set of rules governing packet-switched computer communications networks).

after he logged into a child pornography website.[8] While ultimately relying on the good faith exception[9] to avoid suppressing all evidence against Ammons,[10] the court held that without a valid warrant, the NIT program was a search in violation of the Fourth Amendment.[11] The court reasoned that because the NIT program went into Ammons' personal computer and surreptitiously reprogrammed his computer to elicit his true IP address, the FBI had conducted a search and violated Ammons' reasonable expectation of privacy in his personal computer.[12]

This Case Comment contends that the *Ammons* court ignored case law that more appropriately controlled the Fourth Amendment inquiry. The court should have premised its decision on case law holding that computer code may be considered contraband per se[13] and on case law holding that there is no reasonable expectation of privacy in contraband per se.[14] Additionally, the court should have analyzed case law holding that there is no reasonable expectation of privacy in derivative contraband.[15] The court's decision set a dangerous precedent that rewards tech-savvy child sexual abusers and essentially shuts down a cutting-edge law enforcement tool in the battle to end the sexual abuse of children.

In December 2014, the FBI launched an investigation into Playpen, a website "dedicated to the advertisement and distribution of child pornography" and "the discussion of matters pertinent to child sexual abuse."[16] Playpen functioned not as a regular website available through the open, traditional internet, but as a hidden website on Tor,[17] a software program designed to enable anonymous internet

8. *Ammons*, 207 F. Supp. 3d at 736–37.

9. The good faith exception to suppression of evidence "recognizes that societal costs tend to outweigh the deterrent value of suppression when 'the police act with an objectively "reasonable good-faith belief" that their conduct is lawful, or when their conduct involves only simple, "isolated" negligence.'" *Id.* at 743 (quoting Davis v. United States, 564 U.S. 229, 238 (2011)).

10. *Id.* at 744.

11. *Id.* at 739, 741–42.

12. *Id.* at 739.

13. *See* United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

14. *See* United States v. Emery, 541 F.2d 887 (1st Cir. 1976), *overruled on other grounds by* United States v. Miller, 636 F.2d 850 (1st Cir. 1980). Contraband per se is defined as "[p]roperty whose possession is unlawful regardless of how it is used." *Contraband: Contraband Per Se*, Black's Law Dictionary (10th ed. 2014).

15. *See* United States v. Jones, 31 F.3d 1304 (4th Cir. 1994). Derivative contraband is defined as "[p]roperty whose possession becomes unlawful when it is used in committing an illegal act." *Contraband: Derivative Contraband*, Black's Law Dictionary (10th ed. 2014).

16. *Ammons*, 207 F. Supp. 3d at 735–37 (citation omitted).

17. *Id.* at 736. The technology behind Tor's core principle of internet anonymity was originally funded and developed by the U.S. Office of Naval Research in 1995 and was further developed by the Defense Advanced Research Projects Agency. Joseph Babatunde Fagoyinbo, The Armed Forces: Instrument of Peace, Strength, Development and Prosperity 262 (2013). Tor emerged as a direct result of those research efforts. *Id.* Today, Tor is funded and engineered by the Tor Project, a non-profit organization. *Tor FAQ: What Is Tor?*, Tor, https://www.torproject.org/docs/faq.html.en#WhatIsTor (last visited Apr. 10, 2018).

communication by shrouding the IP addresses of users and website operators alike.[18]

When a user on the open internet enters a web address into her browser, the request and her IP address are sent to a local router[19] owned by an internet service provider (ISP).[20] The router examines the request and determines where the request should be sent.[21] Instead of forwarding the user's IP address with the request, the ISP will send out that router's IP address with the request to the final destination server, where the website is hosted.[22] Generally, a website will maintain logs of all router IP addresses that access that website.[23] Because a user's IP address is not disseminated past the ISP's router, it is the ISP's router IP address that is actually logged and not the user's computer IP address.[24]

Once received by the destination server, the request to visit a website is executed, and, using the router's IP address,[25] it sends packets (small chunks of information and code that make up the website) back to the ISP's router.[26] Once the packets are returned to the user's computer, her web browser renders the code as a visual web page.[27]

To conceal a user's IP address, Tor masks the request to visit a website.[28] Once the IP address passes through the ISP's router, Tor sends the request through a

---

18. *Ammons*, 207 F. Supp. 3d at 736.

19. A router is a device linked to connection points in a network for the transfer of data between computers. *See* Achyut Godbole & Atul Kahate, Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing 35 (3d ed. 2013).

20. *See* Mozilla, *How Does the Internet Work?*, MDN Web Docs, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/How_does_the_Internet_work (last updated Oct. 19, 2017, 9:28:41 AM).

21. Rus Shuler, How Does the Internet Work? § 6 (2005).

22. *See* Weissman, *supra* note 7.

23. *Ammons*, 207 F. Supp. 3d at 736.

24. Weissman, *supra* note 7. If law enforcement assumes control of a website, it can access the log of router IP addresses that visited the website. *Ammons*, 207 F. Supp. 3d at 736. Law enforcement could then ascertain which ISP owns the local router IP address and subpoena the ISP for the account holder's identity and address linked to the user IP address that made the request. *Id.*

25. An IP address functions like a return address on a letter. Brian Komar et al., Firewalls for Dummies 37 (2d ed. 2003).

26. Eric Raymond, The Unix and Internet Fundamentals HOWTO § 12.3 (2010), http://www.tldp.org/HOWTO/pdf/Unix-and-Internet-Fundamentals-HOWTO.pdf. *See generally* Info. Scis. Inst., *supra* note 7 (providing background on fundamental concepts of IP addresses); *Understanding TCP/IP Addressing and Subnetting Basics*, Microsoft, https://support.microsoft.com/en-us/kb/164015 (last visited Apr. 10, 2018) (explaining how an IP address functions).

27. Mozilla, *How the Web Works*, MDN Web Docs, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last updated Aug. 11, 2017, 11:45:55 PM).

28. Using Tor, the only information that the ISP can see from the request is the user's individual IP address and that the user is running Tor, as opposed to when browsing on the open, traditional web, where the ISP can see both the user's individual IP address and the specific site the user is trying to visit. *See Tor FAQ: What Protections Does Tor Provide?*, Tor, https://www.torproject.org/docs/faq.html.en#WhatProtectionsDoesTorProvide (last visited Apr. 10, 2018); *see also* Dune Lawrence, *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built*, Bloomberg Businessweek (Jan. 23, 2014, 8:51 PM), http://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-

network of thousands of volunteer "relay computers" before reaching the destination server.[29] As the request passes through each relay computer, the IP address sent along with the request changes to that of each relay computer.[30] This ensures that the only IP address revealed to the destination website is that of the last computer in the network of relay computers.[31] There is no way to trace the route of the request back through the relay computer network to reveal the local router IP address.[32]

Not only must the user access a hidden website through Tor, but once in Tor, she must also know the precise Tor address of the hidden website to arrive at that website.[33] A user can obtain the exact address through word of mouth from other users of that hidden website or through "online postings describing both the sort of content available on [the hidden website] and its location."[34]

During the investigation into Playpen, the FBI managed to trace the hidden website to a server in North Carolina.[35] The FBI transported the website to a government-controlled server in Virginia, then assumed control of Playpen.[36] Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia issued a warrant ("NIT warrant") for the FBI to deploy the NIT on Playpen's server.[37]

The NIT, a "series of code that instructed a user's computer to transmit certain information to the FBI after the user logged on to Playpen," was deployed by the FBI in an attempt to identify Playpen users instead of shutting down the website.[38] When a computer is operating with an obscured IP address on Tor, the NIT functions by augmenting the code contained in the packets that are sent back to a user's computer.[39] Once the NIT is transmitted in those packets from the website to

agency#p3; *How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy*, Electronic Frontier Found., https://www.eff.org/pages/tor-and-https (last visited Apr. 10, 2018) (displaying, through an interactive diagram, the data available to "eavesdroppers" when using Tor).

29. *Tor FAQ: What Is Tor?*, *supra* note 17.

30. *Tor: Overview*, Tor, https://www.torproject.org/about/overview (last visited Apr. 10, 2018).

31. United States v. Ammons, 207 F. Supp. 3d 732, 736 (W.D. Ky. 2016).

32. *Id.*

33. *Id.* A user cannot use a search engine to search for or stumble across the hidden website. *Id.* Common search engines include Google, Bing, Yahoo!, and Ask. *Webwise: What Is a Search Engine?*, BBC, http://www.bbc.co.uk/webwise/0/22562913 (last updated June 6, 2013, 6:53 PM).

34. Defendant's Motion to Suppress Evidence & Statements at 140, *Ammons*, 207 F. Supp. 3d 732 (No. 3:16-CR-00011).

35. *Ammons*, 207 F. Supp. 3d at 737.

36. *Id.*

37. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 114–17.

38. *Ammons*, 207 F. Supp. 3d at 737.

39. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 106.

the user's computer, the code instructs the computer to transmit the user's actual IP address[40] to a government-controlled computer.[41]

The NIT revealed that on March 4, 2015, an account with the username "H8RL3Y" registered on Playpen and "accessed several images of child pornography over a six-hour period of activity."[42] The FBI traced the IP address to a Kentucky address, where Dennis Ammons resided.[43]

The FBI then obtained and executed a search warrant from a judge in the Western District of Kentucky to search Ammons' residence for evidence of child pornography.[44] Ammons admitted to officers that he had viewed child pornography,[45] and he was arrested and indicted for knowingly producing and receiving child pornography.[46]

Ammons filed a Motion to Suppress, seeking to exclude "all information seized pursuant to the NIT warrant, including the evidence obtained during or as a result of the search of his home."[47] Ammons argued that Judge Buchanan in Virginia did not have jurisdiction[48] to issue the NIT warrant for a computer in Kentucky.[49] Ammons asserted that without a valid NIT warrant, the FBI's search of his computer violated his Fourth Amendment right to be free from unreasonable searches and seizures.[50] Ammons further argued that the good faith exception should not apply, as it was not objectively reasonable for the FBI to believe that the NIT warrant was properly issued.[51]

---

40. The NIT program also may obtain the user's operating system username, host name, active operating system username, media access control address, and unique identifier. *Ammons*, 207 F. Supp. 3d at 737. That the NIT program was able to obtain these elements, though, was not contested or at issue in this case. *See id.* at 739–40.

41. *See id.* at 737.

42. *Id.*

43. *Id.* Ammons' sister and her two minor children, "Jane Doe" and "Jane Roe," also lived at the Kentucky address. *Id.*

44. *Id.* at 737.

45. Subsequently, on December 29, 2015, the FBI observed an interview with Jane Doe, who recounted an episode in which "Ammons made her pose fully nude in the 'spread-eagle' position on his bed while he photographed her" and "multiple occasions when Ammons forced her to completely undress and sit on his bed 'with her legs open while facing Ammons and his computer.'" *Id.* at 737–38 (citation omitted).

46. *Id.* at 738.

47. *Id.*

48. Judge Buchanan's jurisdictional limits are defined by the Federal Magistrates Act and Federal Rule of Criminal Procedure 41(b). *Id.* at 740. The Federal Magistrates Act grants magistrate judges "all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1) (2012). Rule 41(b)(1) grants magistrate judges "authority to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1).

49. *Ammons*, 207 F. Supp. 3d at 737–38.

50. *Id.* at 738.

51. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 66.

The government argued in response that use of the NIT was not a search because there is no reasonable expectation of privacy in IP addresses.[52] Alternatively, the government argued that if the court found use of the NIT to be a search, the search would be reasonable even without a valid warrant because of exigent circumstances[53] of the "'ongoing abuse' of children."[54] Lastly, the government asserted that suppression of the evidence would be inappropriate because the FBI conducted the search in good faith reliance on the NIT warrant.[55]

The court held that use of the NIT was a Fourth Amendment search that required a valid warrant.[56] However, the court found that Judge Buchanan lacked the authority to issue the NIT warrant.[57] The court ultimately ruled that while the search of Ammons' computer constituted a warrantless search in violation of the Fourth Amendment, the good faith exception applied, and therefore, suppression of the evidence was not an appropriate remedy.[58]

In determining that use of the NIT amounted to a search, the court articulated that a search occurs whenever the government "'invades an individual's reasonable expectation of privacy' in the place or thing to be searched."[59] To define a search, the court relied on a two-prong test requiring that (1) a person exhibit an "actual and subjective expectation of privacy in the thing to be searched or seized," and (2) the subjective expectation be objectively reasonable according to society.[60] The court reasoned that there was no dispute over Ammons' subjective expectation of privacy in the contents of his personal computer,[61] and his expectation of privacy was objectively reasonable because "[g]enerally speaking, computer users have a reasonable expectation of privacy in data stored on a home computer."[62]

---

52. *Ammons*, 207 F. Supp. 3d at 739.

53. Exigent circumstances have been defined as "when officers 'have probable cause to believe that evidence of illegal activity is present and [ ] reasonably believe that evidence may be destroyed or removed before they could obtain a warrant' . . . or when 'speed is essential to prevent escape or harm to police or others.'" United States' Response to Motion to Suppress at 182, *Ammons*, 207 F. Supp. 3d 732 (No. 3:16-CR-11) (alteration in original) (first quoting United States v. Cephas, 254 F.3d 488, 494–95 (4th Cir. 2001); then quoting Mora v. City of Gaithersburg, 519 F.3d 216, 226 (4th Cir. 2008)).

54. *Ammons*, 207 F. Supp. 3d at 742 (citation omitted).

55. *Id.* at 743.

56. *Id.* at 738–39. The court began its analysis with the inquiry of whether use of the NIT constituted a search; if the court found that use of the NIT did not constitute a search, then no warrant would be necessary, and the analysis would stop there. If it found that use of the NIT was a search, as it did here, then a valid warrant would be necessary, unless an exception to the warrant requirement applied. *See id.*

57. *Id.* at 738, 740. The court reasoned that Judge Buchanan's NIT warrant authorized a search of property in Kentucky, located outside her judicial district. *Id.* at 740.

58. *See id.* at 739–44.

59. *Id.* at 738–39 (quoting United States v. Anderson-Bagshaw, 509 F. App'x 396, 402 (6th Cir. 2012)).

60. *Id.* at 739 (citing United States v. Mathis, 738 F.3d 719, 729 (6th Cir. 2013)).

61. *Id.*

62. *Id.* (quoting United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013)).

This Case Comment contends that while the U.S. District Court for the Western District of Kentucky ultimately came to the correct holding using the good faith exception, the court erred in finding that use of the NIT constituted a search under the Fourth Amendment because the court completely ignored case law that more appropriately controlled this case. The court failed to analyze relevant case law holding that computer code containing instructions to view child pornography may constitute contraband,[63] alongside case law holding that there is no reasonable expectation of privacy in contraband per se[64]—or property whose possession is unlawful regardless of how it is used.[65] Additionally, the court failed to analyze relevant case law holding that there is no reasonable expectation of privacy in derivative contraband.[66] If the court had applied the correct case law, use of the NIT would not constitute a search within the meaning of the Fourth Amendment. This decision sets a dangerous precedent that rewards tech-savvy child sexual abusers and essentially shuts down a cutting-edge law enforcement tool in the battle to stop the sexual abuse of children.

First, the court erred because it failed to consider that there is no objectively reasonable expectation of privacy in contraband per se. Instead, the court incorrectly reasoned that the defendant had a reasonable expectation of privacy in data stored on his computer, simply stating that "[g]enerally speaking, computer users have a reasonable expectation of privacy in data stored on a home computer."[67] However, the packets Ammons received from visiting Playpen contained contraband per se, or property which he had no legal right to possess.[68] Federal law prohibits any person from knowingly receiving or distributing "any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer."[69] Child pornography is defined as a visual depiction involving a minor engaging in sexually explicit conduct;[70] a visual depiction may include "data stored on [a] computer disk or by electronic means [that] is capable of conversion into a visual image, and data which is capable of conversion

63. *See* United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

64. *See* United States v. Emery, 541 F.2d 887, 890 (1st Cir. 1976), *overruled on other grounds by* United States v. Miller, 636 F.2d 850 (1st Cir. 1980).

65. *Contraband: Contraband Per Se*, Black's Law Dictionary, *supra* note 14.

66. *Contraband: Derivative Contraband*, Black's Law Dictionary, *supra* note 15. *See* United States v. Jones, 31 F.3d 1304 (4th Cir. 1994).

67. United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016) (quoting United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013)). However, *Conner* discusses whether law enforcement, in person, viewing content already on a computer constitutes a search. *Conner*, 521 F. App'x at 494–98. The *Ammons* court misses the mark; *Conner* is inapplicable as it does not discuss tracking illegal content that does not originate on a private computer.

68. *Contraband: Contraband Per Se*, Black's Law Dictionary, *supra* note 14.

69. 18 U.S.C. § 2252A(a)(2)(B) (2012).

70. *Id.* § 2256(8)(A)–(C).

into a visual image that has been transmitted by any means, whether or not stored in a permanent format."[71] In instances when the code contains instructions to view child pornography, the code is comprised of "data which is capable of conversion into a visual image."[72]

In *United States v. Romm*, the court considered whether a defendant, who had viewed websites containing child pornography, received child pornography when his computer automatically saved copies of the image files to his internet cache.[73] The defendant argued that files in the internet cache were not visual depictions constituting child pornography because the files are comprised of data in an unviewable form until the user takes the additional step of converting the data into ordinary image files.[74] The court rejected this argument, stating that the law "speaks of data files that are *capable* of conversion into a viewable form, not data files that are immediately viewable without any further affirmative steps."[75]

Here, to view the website on his browser, Ammons intentionally downloaded the packets of information that contained the instructions to view the child pornography in his browser.[76] The code in this case, while only temporarily on his computer, was not only capable of conversion into a viewable form like in *Romm*, but actually did convert the data into viewable form.[77] Therefore, just as in *Romm*, the code itself was child pornography, or contraband per se, in which Ammons had no objectively reasonable expectation of privacy.

Furthermore, in *United States v. Emery*, Drug Enforcement Agents, without a warrant, placed an electronic beeper[78] in two packages intercepted by customs

71. *Id.* § 2256(5).

72. *See* United States v. Lynn, 636 F.3d 1127, 1135 & n.8 (9th Cir. 2011) ("[W]hen Congress enacted § 2252(a)(2) and (a)(4)(B), it criminalized the receipt, distribution, and possession of images and videos of child pornography, regardless of the format or media in which such images were captured when the offender was caught. As we explained in a different context: 'The visual image transported in binary form starts and ends pornographically and that is what Congress seeks to prohibit.'" (quoting United States v. Hockings, 129 F.3d 1069, 1072 (9th Cir. 1997))).

73. 455 F.3d 990, 997–1002 (9th Cir. 2006). An internet cache is a temporary storage place on a web user's browser for data that has already been requested or accessed by the user. ViSolve, Optimized Bandwidth + Secured Access = Accelerated Data Delivery 4 (2009), http://www.visolve.com/uploads/resources/ViSolve_Web_Caching.pdf.

74. *Romm*, 455 F.3d at 998. The distinction between computer code and data in an unviewable form is insignificant in this context and does not affect this argument.

75. *Id.* at 998–99.

76. *See* United States v. Ammons, 207 F. Supp. 3d 732, 737 (W.D. Ky. 2016).

77. *See id.*

78. A beeper is a "radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver" that law enforcement can use in tracking the item to which the beeper is attached. United States v. Knotts, 460 U.S. 276, 277 (1983).

agents.[79] Each package contained a sound speaker and cocaine.[80] The defendant then picked up his packages, and agents followed him back to his apartment where they maintained surveillance and monitored the beeper's signal.[81] The court considered whether the warrantless insertion of the beeper into the packages violated the Fourth Amendment.[82] The court held that this was not a Fourth Amendment violation because "the beeper was not attached to [the defendant's] car (nor to his person, nor to an object legitimately possessed by him); rather, it was inserted into a package containing *contraband*, property which he had no right to possess."[83] Since the defendant had no objectively reasonable expectation of privacy in the contraband per se, there was no violation of his Fourth Amendment right to be free from unreasonable searches and seizures.[84]

In *Ammons*, the code in the packets constituted contraband per se, and just like in *Emery*, there is no objective expectation of privacy in contraband per se.[85] When the Playpen web address was entered into a browser, the first landing page for the login screen overtly displayed two images "depicting partially clothed prepubescent females with their legs spread apart."[86] This means that the packets sent from the server to Ammons' computer contained instructions and code to display child pornography—the packets themselves contained contraband. When the defendant knowingly and intentionally accessed the landing page and then logged into the website,[87] the government deployed the NIT program by embedding the NIT code in the code of those packets.[88] Once in the computer, the NIT sent back the actual IP address of

79. 541 F.2d 887, 888 (1st Cir. 1976), *overruled on other grounds by* United States v. Miller, 636 F.2d 850 (1st Cir. 1980).

80. *Id.*

81. *Id.*

82. *Id.* at 889.

83. *Id.* at 889–90; *accord* United States v. Bailey, 628 F.2d 938, 942 (6th Cir. 1980) (noting a line of cases where installing beepers in contraband was not a Fourth Amendment search because society does not recognize an expectation of privacy in contraband); United States v. Washington, 586 F.2d 1147, 1154 (7th Cir. 1978) (holding that attaching a beeper to a package of cocaine was not a Fourth Amendment search as the defendant had no reasonable expectation in a package of contraband); United States v. Moore, 562 F.2d 106, 111 (1st Cir. 1977) (determining that placement of beepers in legally possessed items constitutes a search, as opposed to placement of beepers in contraband substances), *abrogation recognized by* United States v. Oladosu, 744 F.3d 36 (1st Cir. 2014).

84. *Emery*, 541 F.2d at 890.

85. *See id.* at 889–90.

86. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 95.

87. Playpen could not be "stumbled upon" on the open internet; accessing the hidden site required numerous affirmative steps by the user, making it virtually *impossible* to get to the site without knowing its content and purpose. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 94–95; *see* United States v. Ammons, 207 F. Supp. 3d 732, 736–37 (W.D. Ky. 2016). Furthermore, the government waited until a user affirmatively logged into Playpen using a registered username and password before deploying the NIT. *Id.* at 737.

88. Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 106.

Ammons' computer to a computer controlled by the FBI.[89] This situation is directly analogous to *Emery*, in which law enforcement placed a beeper in a package of contraband per se and allowed the defendant to transport the package to another location, whereupon the beeper sent back the location of the contraband per se.[90]

Had the court applied the holdings of *Romm* and *Emery* to the facts of *Ammons*, it would be apparent that the code was contraband per se, and thus Ammons had no objectively reasonable expectation of privacy in the code. Therefore, embedding the NIT program into the code and allowing the NIT to send back Ammons' true IP address did not amount to a search in violation of the Fourth Amendment.

Second, even if the *Ammons* court determined that the code itself was not contraband per se, the court still failed to analyze other relevant case law that would show that use of the NIT was not a Fourth Amendment search. Because there is no objectively reasonable expectation of privacy in derivative contraband,[91] or property whose possession becomes unlawful when it is used in committing an illegal act,[92] there was no search performed. Here, the code belonging to the government was used to display an illegal website.[93] When Ammons accessed the website and transmitted the code, he was taking possession of code used to commit an illegal act and consequently had no objectively reasonable expectation of privacy in that code.

In *United States v. Jones*, law enforcement suspected the defendant of stealing postal service deposit envelopes containing a total of $17,000 from mail pouches.[94] Officers placed a beeper in a deposit envelope addressed to a bank inside a mail pouch.[95] Law enforcement did not witness the defendant place the mail pouch in his van, but tracked the beeper to the defendant's van.[96] He was then indicted for theft of United States Mail.[97]

The defendant claimed use of the beeper was a warrantless search in violation of the Fourth Amendment, because when the monitoring of a beeper "reveals a 'critical fact about the interior' of the premises that could not have been obtained through visual surveillance," it "falls within the ambit of the Fourth Amendment."[98] He argued

89. *Ammons*, 207 F. Supp. 3d at 737.

90. *Emery*, 541 F.2d at 888.

91. *See* United States v. Jones, 31 F.3d 1304, 1311 (4th Cir. 1994); *see also* United States v. Perez, 526 F.2d 859 (5th Cir. 1976) (holding that the defendant had no reasonable expectation of privacy in a television set, received in exchange for heroin, that was tracked by a beeper to the defendant's car); Nored v. State, 875 S.W.2d 392 (Tex. Crim. App. 1994) (holding that the defendant had no reasonable expectation of privacy in a stolen bicycle that was tracked by a beeper back to the defendant's fenced-in yard).

92. *Contraband: Derivative Contraband*, Black's Law Dictionary, *supra* note 15.

93. *Ammons*, 207 F. Supp. 3d at 737.

94. 31 F.3d at 1307.

95. *Id.*

96. *Id.* at 1308.

97. *Id.*

98. *Id.* at 1308–10 (citing United States v. Karo, 468 U.S. 705, 715–16 (1984)).

that a critical fact was that the envelope was inside the van,[99] and concealing personal property from public view normally gives rise to Fourth Amendment protections.[100] The court acknowledged this, but held that because the beeper was placed in the envelope, which was owned by the government, the defendant had no reasonable expectation of privacy in the envelope, even if it meant that the beeper revealed the envelope's ultimate location inside of the van.[101] The court stated that "[t]he mail pouch with the beeper found its way into [the defendant's] van only because [the defendant] stole the pouch and hid it in the van himself," and "what was concealed from public view was not personal property, it was stolen government property."[102] Although envelopes themselves are not illegal to possess, the envelope became illegal to possess when it was used to commit a crime—the envelope became derivative contraband. Consequently, law enforcement's actions did not amount to a search.[103]

Had the *Ammons* court followed the reasoning in *Jones*, it would have found that Ammons had no objectively reasonable expectation of privacy in derivative contraband. Even if the court was to find that the code constituting child pornography was not contraband per se, it became derivative contraband when used in the commission of a criminal act. The illegal website and all the code composing the website belonged to the government.[104] Just as the beeper in *Jones* was placed in the government's envelope, the NIT program was placed in the government's code.[105] In the same way that the beeper revealed that the envelope ended up inside the defendant's van because he placed the envelope there,[106] the NIT program revealed that the code ended up inside Ammons' computer only because Ammons logged into the website and requested that the government's code be transmitted to his computer.[107] Had the court applied the *Jones* reasoning to *Ammons*, it would be clear that Ammons had no objectively reasonable expectation of privacy in the code as derivative contraband. Thus, embedding the NIT program into the code and allowing the NIT to send back Ammons' true IP address did not amount to a search in violation of the Fourth Amendment.

The Fourth Amendment no doubt protects concerns of the utmost importance. Our Founding Fathers baked into the very language of our Constitution the right to remain free from unreasonable governmental overreach and to feel safe and secure in the privacy of our own homes.[108] Yet, the type of privacy rights the Fourth

99. *Id.* at 1308.

100. *Id.* at 1310.

101. *Id.*

102. *Id.*

103. *Id.* at 1310–11.

104. *See* United States v. Ammons, 207 F. Supp. 3d 732, 737 (W.D. Ky. 2016).

105. *Jones*, 31 F.3d at 1310; Defendant's Motion to Suppress Evidence & Statements, *supra* note 34, at 106.

106. *See Jones*, 31 F.3d at 1310.

107. *See Ammons*, 207 F. Supp. 3d at 737.

108. *See* U.S. Const. amend. IV.

Amendment was intended to protect are not at issue here—the Fourth Amendment was not created to protect the guilty.[109]

"It is easier to build strong children than to repair broken men."[110] The potential privacy interests in this case are minimal compared to the societal harm that results from failing to prevent the spread of child pornography. Child victims not only suffer at the physical hands of their abusers who sexually exploit them, but every time photos and videos of the abuse are distributed, viewed, and downloaded, the child is re-victimized.[111]

By finding that the NIT is a Fourth Amendment search that requires a warrant, the *Ammons* court is effectively rewarding tech-savvy child sexual abusers, encouraging them to continue to advance their criminal technologies,[112] and preventing law enforcement from using a powerful tool in helping to combat those abusers. It is imperative that the judicial system understand the minute details of how technology functions in order to effectively apply laws that were created before the internet was even fathomable.[113]

The *Ammons* court failed to analyze relevant case law holding that there is no reasonable expectation of privacy in contraband per se and that code may constitute contraband. Additionally, the court failed to analyze relevant case law holding that there is no reasonable expectation of privacy in derivative contraband, regardless of the final destination of that contraband. Had the court applied the correct case law, use of the NIT would not have constituted a search within the meaning of the

---

109. *The Jury and the Search for Truth: The Case Against Excluding Relevant Evidence at Trial: Hearing on S. 3 Before the S. Comm. on the Judiciary*, 104th Cong. 58 (1995) (statement of Paul J. Larkin, Jr., King & Spalding LLP).

110. Charles M. Blow, Opinion, *Fathers' Sons and Brothers' Keepers*, N.Y. Times, Mar. 1, 2014, at A19 (quoting Frederick Douglass).

111. *See generally Sexual Exploitation of Children over the Internet: What Parents, Kids and Congress Need to Know About Child Predators: Hearings Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 109th Cong. 256 (2006) (statement of William W. Mercer, Principal Associate Deputy Att'y Gen., U.S. Dep't of Justice). Many activists refer to child pornography as "crime scene photographs" to emphasize the photograph as a permanent record of the abuse of a child. *See Defining Child Pornography*, Stop It Now!, http://www.stopitnow.org/ohc-content/defining-child-pornography (last visited Apr. 10, 2018).

112. In 2011, Attorney General Eric Holder stated:

> [U]nfortunately, . . . we've . . . seen an historic rise in the distribution of child pornography, in the number of images being shared online, and in the level of violence associated with child exploitation and sexual abuse crimes. Tragically, the only place we've seen a decrease is in the age of victims. This is unconscionable—and it is unacceptable.

Eric Holder, Att'y Gen., U.S. Dep't of Justice, Remarks at the National Summit on Protecting Children from Sexual Exploitation (Oct. 14, 2011), https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-national-summit-protecting-children-sexual.

113. The Founding Fathers signed the U.S. Constitution using quill pens in 1787. *See* 1 John R. Vile, The Constitutional Convention of 1787, at *lv* (2d. ed. 2016). The World Wide Web was invented in 1990. Evan Andrews, *Who Invented the Internet?*, History (Dec. 18, 2013), http://www.history.com/news/ask-history/who-invented-the-internet.

Fourth Amendment. The dangerous precedent left by this decision leads our society one step away from building strong children, and one step closer to having to repair broken men and women.