Volume 63
Issue 6 *V.63, Tolle Lege*

Article 5

6-15-2019

You've Got Mail: FBI Hacking in United States v Lough and Why It Is a Fourth Amendment Search

Ryan Dieter

YOU'VE GOT MAIL: FBI HACKING IN *UNITED STATES v. LOUGH* AND WHY IT IS A FOURTH AMENDMENT SEARCH

RYAN DIETER*

"[This] can lead to large-scale privacy and civil liberties abuses at home and abroad."[1]

I. PLUGGING IN: REVISITING THE DEBATE BETWEEN SECURITY AND PRIVACY

The Inland Regional Center is a facility for those with developmental disabilities.[2] Until December 2, 2015, most people had never heard of the San Bernardino facility, but on that date, it became the infamous location of one of the most memorable and devastating terrorist attacks on American soil.[3] The shooters, Syed Farook and his wife Tashfeen Malik, killed fourteen people and wounded twenty-two others.[4] Perhaps even more well-known than the actual attack was the Federal Bureau of Investigation's (FBI) extremely public battle with Apple over access to Farook's iPhone.[5]

After seizing the smartphone, the FBI realized that Farook had secured the

---

* J.D. Candidate, 2019, Villanova University Charles Widger School of Law; B.A. 2016, The Pennsylvania State University. This Note is dedicated to my family, friends, and all those who have supported me throughout my life. I would also like to extend a special thanks to everyone on the *Villanova Law Review* for all of their contributions.

1. *See* Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, WASH. POST (Jan. 21, 2016), https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html?utm_term=.aa634855ec1e [https://perma.cc/HZ8S-7DRY] (quoting Ahmed Ghappour, professor at University of California's Hastings College of the Law).

2. *See* Mark Schone et al., *San Bernardino Shooting: What Is the Inland Regional Center?*, NBC NEWS (Dec. 2, 2015), https://www.nbcnews.com/sToryline/san-bernardino-shooting/san-bernardino-shooting-what-inland-regional-center-n473016 [https://perma.cc/TWT8-NHDH] ("The site of a deadly mass shooting in San Bernardino, California . . . had just held a holiday party a day before the shots rang out.").

3. *See* Wm. Robert Johnston, *Terrorist Attacks and Related Incidents in the United States*, JOHNSTON'S ARCHIVE, http://www.johnstonsarchive.net/terrorism/wrjp255a.html [https://perma.cc/CHK2-L8VE] (last visited Mar. 24, 2018) (providing compilation of all incidents of terror in the United States since 1865); *Everything We Know About the San Bernardino Terror Attack Investigation*, THE SUN (Nov. 27, 2016, 04:05 PM), http://www.sbsun.com/2016/11/27/everything-we-know-about-the-san-bernardino-terror-attack-investigation/ [https://perma.cc/5PYX-3C94] [hereinafter *Everything We Know*] ("The Dec. 2 shooting at the Inland Regional Center . . . saw a massive response from law enforcement agencies from throughout the region, along with the FBI.").

4. *See Everything We Know*, *supra* note 3 ("[The shooters] died in a gunfight with law enforcement . . . about five hours after the massacre."). Farook was a United States citizen, but his wife came to the country in 2014. *See id.* The only evidence of their radical views was "a Facebook statement in support of terrorist organization Islamic State around the time of the shootings." *See id.* "The couple had drawn a flat line with only a violent spike at the end for investigators to pick apart." *Id.*

5. *See id.* (stating FBI seized "pipe bombs, bomb-making materials and thousands of rounds of ammunition" during a warranted search of the shooters' home). The cellphone was found in Farook's mother's vehicle. *See id.*

device using a passcode.[6] Consequently, if the agents entered the wrong code too many times, the data on the iPhone would be permanently erased.[7] Rather than press their luck, the FBI agents working the case obtained an order from a federal magistrate judge instructing Apple to construct a "backdoor entry" into the iPhone via new software.[8] Apple's Chief Executive Officer, Tim Cook, referred to the federal order as "chilling," comparing the potential software to "a master key, capable of opening hundreds of millions of locks."[9] The technology giant, as well as many other private citizens and commentators, worried that if this unprecedented power were given to the FBI, there would be nothing to stop it from using the software to access countless other phones.[10] Nevertheless due to third party intervention, the FBI was able to unlock the phone before the data was destroyed.[11]

Although debate surrounding the above case was fierce, it represented but one battle in the struggle between the government's interest in effective and efficient law enforcement and the common interest in privacy.[12] Indeed, the framers of the United States Constitution anticipated this friction when they penned the Fourth Amendment's protections against governmental intrusions.[13] Fourth Amendment jurisprudence is well defined for searches occurring in the physical world.[14] However, the rules for electronic searches are far less

6. *See id.* (explaining that Farook had private passcode for iPhone).

7. *See id.* ("[A]gents were concerned they would permanently lose any data on [the phone] if they failed too many times to open it."). The phone was issued to Farook by his employer, San Bernardino County. *See id.* However, the passcode he used to secure the phone had not been shared with county officials. *See id.* With the only person who knew the code dead, the FBI could only make guesses at the correct passcode. *See id.*

8. *See id.* ("[A] federal magistrate in Riverside [issued] an order in February for Apple engineers to develop software for a backdoor entry to the phone.").

9. *See* Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 06:34 AM), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html [http://perma.cc/K94G-GY6X] ("Cook's argument was that if the FBI could access this iPhone, nothing would stop them from doing it to many others.").

10. *See id.* (explaining that data privacy is a sensitive subject after Edward Snowden revealed the extent of surveillance conducted by government).

11. *See id.* (explaining FBI has refused to reveal identity of third party or method used to unlock phone, but some reported the secret partner was Israeli firm called Cellebrite).

12. *See id.* ("The case marked one of the highest-profile clashes in the debate over encryption and data privacy between the government and a technology company."). The government makes a compelling case that encryption methods used in today's technology makes it harder for it to investigate and solve cases. *See id.* Private companies retorted, stating, "encryption is key to protecting user data from hackers." *See id.*

13. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated . . . .").

14. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 351 (2009) (permitting law enforcement to search vehicles incident to arrest); Kyllo v. United States, 533 U.S. 27, 27 (2001) (holding that police may not use thermal camera to look inside suspect's home without warrant); California v. Acevedo, 500 U.S. 565, 565 (1991) (holding that police may search vehicle without warrant, so long as they have probable cause to believe evidence of crime will be found within); Florida v. Riley, 488 U.S. 445, 451 (1989) (holding that there was no violation of Fourth Amendment when police looked down into suspect's fenced-in backyard from helicopter); California v. Greenwood, 486 U.S. 35, 35 (1988) (holding that act of combing through suspect's trash on curb is not search under Fourth Amendment); Chimel v. California,

refined.[15]

Compounding this disparity is the fact that the rapid advancement of investigative technology has granted the FBI the capability to implant what amounts to malware, otherwise known as dangerous software, on a suspect's computer for the purpose of obtaining identifying information about the suspect.[16] This new tactic, known as a network investigative technique (NIT), presented the question at issue in *United States v. Lough*:[17] whether the NIT a Fourth Amendment "search."[18] Courts across the country, including *Lough*, have answered this question in the negative simultaneous with the rise in NIT has an investigative technique.[19] Far fewer cases have found that the NIT is a Fourth Amendment search.[20] Regardless of the varied dispositions, not a single court addressing the issue has completed the search analysis prescribed in the Supreme Court's most important search and seizure case, *United States v. Jones*.[21] In *Jones*, the Court stated that, contrary to previous opinions, whether the government had "physically intruded" into the defendant's privacy is still a crucial part of the determination of whether a Fourth Amendment search had

---

395 U.S. 752, 766–67 (1969) (explaining that police are allowed to conduct limited search incident to arrest); Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (holding that under certain circumstances police may stop and frisk suspect).

15. Just three years ago, in a case determining whether police may search the data on a cell phone, the Supreme Court recognized a difference between a cell phone and a cigarette carton as a container of information. *See* Riley v. California, 134 S. Ct. 2473, 2478–79 (2014) (holding that although cellphones and cigarette cartons can both feasibly hold information, the volume of data a cellphone is capable of storing distinguishes it from all other containers).

16. *See* United States v. Lough, 221 F. Supp. 3d 770 (N.D. W. Va. 2016) (presenting issue of FBI utilizing malware to force suspect's computer to send suspect's IP address and other information to law enforcement agents).

17. 221 F. Supp. 3d 770 (N.D. W. Va. 2016).

18. *See id.* at 774–75 (stating that initial question in deciding whether to suppress evidence is whether a Fourth Amendment search was conducted).

19. *See id.* at 775–76 (holding that because defendant had no reasonable expectation of privacy in information taken by malware, NIT was not a search); *see also* United States v. Jean, 207 F. Supp. 3d 920, 933 (W.D. Ark. 2016) ("[T]he FBI in the instant case was under no legal obligation to obtain a search warrant . . . as IP addresses are unlikely to be entitled to the same Fourth Amendment protections as are the substantive contents of users' computers."); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC2016, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016) (proclaiming that NIT was not search); United States v. Eure, No. 2:16cr43, 2016 WL 4059663, at *9 (E.D. Va. July 28, 2016) (holding that "searches and seizures perform[ed] pursuant to the NIT did not violate Fourth Amendment"); United States v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016) (holding that defendant's computer was not searched because the defendant had no reasonable expectation of privacy in their IP address).

20. *See* United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) (finding that because government "invaded the contents of the computer" NIT constituted Fourth Amendment search); *see also* United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016) (citing United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2010) (holding that because defendant had reasonable expectation of privacy in a computer, rather than a IP address, government's intrusion was a search)); United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016) (holding that installation of code without permission is search).

21. 565 U.S. 400, 409 (2012) (stating that test for whether search has occurred does not end with "reasonable expectation of privacy" examination, but also must include "physical intrusion" test).

occurred.[22]

This Note argues that because the *Lough* court and its many companions overlooked the *Jones* case, they erred in concluding the NIT was not a Fourth Amendment search.[23] First, this Note will provide a brief overview of the technological aspects that seem to confuse courts.[24] Second, this Note will examine the history of Fourth Amendment searches.[25] Then, this Note will summarize the common nucleus of facts that led to *Lough* and describe the court's reasoning for its conclusion.[26] Finally, this Note will demonstrate that under a complete Fourth Amendment analysis, the FBI's use of the NIT constituted a search.[27]

II. READING THE INSTRUCTIONS: COMPUTER SCIENCE 101 AND THE EVOLUTION OF FOURTH AMENDMENT SEARCHES

In her concurrence in *Jones*, Justice Sotomayor suggested that current law regarding searches may not be able to keep pace with the rate of technological advancement.[28] She noted further that expectations of privacy deemed "reasonable" by society may change with the amount of information publicly available about a person via the Internet.[29] Indeed, confusion amongst judges regarding how technology works has led to some incongruous analogies attempting to reconcile the physical world with the digital world.[30]

A. *Welcome to Class: A Brief Overview of Computer Science Concepts*

Cases like *Lough* require a great deal of technical literacy to understand the

22. *See id.* (stating that "reasonable expectation of privacy" determination supplemented rather than replaced the "physical intrusion" inquiry).

23. *See infra* notes 146-87 and accompanying text for critical analysis of *Lough* decision.

24. *See infra* notes 29–59 and accompanying text for background information on relevant computer science concepts.

25. *See infra* notes 60–105 and accompanying text for overview on the history of Fourth Amendment searches.

26. *See infra* notes 106–25 and accompanying text for information about the facts of *Lough*.

27. *See infra* notes 146–87 and accompanying text for critical analysis of *Lough* decision.

28. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

29. *See id.* at 418 ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.").

30. *See id.* at 420 (Alito, J., dissenting) (comparing GPS tracker to law enforcement agent hiding somewhere inside vehicle to track its movements); *see also* United States v. Lough, 221 F. Supp. 3d 770, 777 (N.D. W. Va. 2016) (citing United States v. Jean, 207 F. Supp. 3d 920, 938 (W.D. Ark. 2016)) (agreeing with courts that have likening method computers use to connect to various websites to act of traveling via car to location of server housing site).

issue, and some courts have proven better than others at describing the technology involved.[31] One key technological term to understand before diving into *Lough* is Internet Protocol Address (IP address).[32] An IP address is an identification number that allows devices to connect to the Internet.[33] A house, business, or other physical property has a street address; similarly, each device capable of accessing the Internet has its own specific IP address.[34] A post office cannot deliver mail if the exact receiving address is not provided.[35] Similarly, in the digital world, data cannot be transmitted over the Internet without knowing which IP address to send the information to.[36]

The average Internet user connects to the Internet via an internet service provider (ISP), which then assigns the user an IP address.[37] Along with the ISP, website administrators can view the IP addresses of all individuals who visit their sites, however, only the ISP can link the IP address to a person's true identity.[38] At least one court has looked into the privacy rights individuals have in their IP addresses.[39] For instance, even in a case where the FBI had administrative control of a website and could see the IP addresses visiting a child pornography website, it was only able to obtain the suspects' names by going to the ISP.[40]

In child pornography cases it is common for users of illicit sites to hide their IP addresses from child pornography websites using software called The

31. *See Jean*, 207 F. Supp. 3d at 924–27 (explaining, in great detail, technology used to hide child pornography websites on Internet and FBI's NIT process).

32. *See Lough*, 221 F. Supp. 3d at 775 (determining that individual does not have reasonable expectation of privacy in an IP address because it has been shared with a third party).

33. *See* Tim Fisher, *What Is an IP Address*, LIFEWIRE (Jun. 1, 2017), https://www.lifewire.com/what-is-an-ip-address-2625920 [https://perma.cc/MSA4-ZR8C] ("Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.").

34. *See id.* ("[D]evices on a network are differentiated from one another through IP addresses.").

35. *See id.* ("It's not enough to just put a package with [the recipient's] name on it through the mail and expect it to reach him.").

36. *See id.* ("[I]nstead of using a phone book to look up someone's name to find their physical address, your computer uses DNS servers to look up a hostname to find its IP address."). A Domain Name System (DNS) server is a database of IP addresses and their common names (i.e. "google.com"). *See* Tim Fisher, *What Is a* DNS Server?, Lifewire (Jan. 16, 2018), https://www.lifewire.com/what-is-a-dns-server-2625854 [https://perma.cc/ZPF2-FJHX] (explaining DNS servers and their relation to IP addresses).

37. *See* United States v. Christie, 624 F.3d 558, 563 (3d. Cir. 2010) (explaining process of customers connecting to the internet). ISPs only keep information on customers' assigned IP address for a short window of time because many ISPs change their customers' IP addresses over time. *See id.* ("Depending on the ISP, a customer's IP address can change each time he logs on to the internet.").

38. *See id.* ("IP addresses are also conveyed to websites that an internet user visits . . . . However, site administrators do not possess information linking a given IP address to a particular person.").

39. *See id.* at 573 (considering whether defendant had reasonable expectation of privacy in his IP addresses).

40. *See id.* (explaining that FBI was only able to learn defendant's legal name by gaining administrative access to site, monitoring IP addresses, and asking ISP to match IP addresses with associated users).

Onion Router (Tor).[41] Tor's name is a nod to the way in which it cloaks users' IP addresses; it "bounces" a user through a network of other Tor users in order to create "layers" of protection.[42] The protection takes away a website's ability to read a user's IP address, only revealing that someone is using Tor to visit the website.[43] Each layer in the chain only knows the prior IP address and the next layer to send it to.[44] As a result, no single layer knows both the real IP address and the target webpage.[45]

Although Tor is commonly used for nefarious purposes, it originated as a way for the United States military to mask its confidential communications.[46] For Tor to be effective, these confidential communications needed to be hidden amongst other, non-military users.[47] This is why Tor is free to download for anyone who wishes to utilize it.[48] Because of its open availability, many use Tor for truly innocent and even humanitarian purposes.[49] Nevertheless, it is also an attractive piece of software for criminals who have created a "Dark Web" filled with child pornography websites and illicit drug markets.[50]

---

41. *See* United States v. Lough, 221 F. Supp. 3d 770, 772 (N.D. W. Va. 2016) (stating that Tor allows criminals to interact with child pornography websites without detection by law enforcement by "hiding their IP addresses and identities"); *see generally*, Abbott, *Hiding from Prying Eyes*, OR. ST. B. BULL. 32 (2008)(concluding that resources like Tor can be used for criminal purposes and "heroic" purposes).

42. *See* NPR Staff, *Going Dark: The Internet Behind the Internet*, NPR: ALL THINGS CONSIDERED (May 25, 2014, 06:54 PM), http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet [https://perma.cc/TF9J-24YC] ("[T]he onion refers to the layers you go through to disguise your identity.").

43. *See id.* (explaining that when using Tor, the location given to website will change to a different node in the Tor network). For instance, a user in Washington, D.C. could send internet traffic across the globe and "the website that [a user visits] will see that someone in Russia is visiting, not [the user] in D.C." *See id.*

44. *See Tor: Overview*, THE TOR PROJECT, https://www.torproject.org/about/overview.html.en [https://perma.cc/AWM7-HFY5] (last visited Sept. 1, 2017) ("No individual relay ever knows the complete path that a data packet has taken.").

45. *See Tor: Overview*, *supra* note 44 ("Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can . . . link the connection's source and destination."). Tor keeps a given circuit open for only ten minutes, then a new circuit is created to ensure anonymity. *See id.* Tor's process has been likened to a skilled getaway driver escaping a "tail" by police. *See id.*

46. *See* NPR Staff, *supra* note 42 (stating that Tor was developed at Naval Research Laboratory).

47. *See id.* ("[B]y opening up this system to everyone, different groups of people can hide in a big crowd of anonymous Tor users.").

48. *See* United States v. Jean, 207 F. Supp. 3d 920, 924 (W.D. Ark. 2016) (describing Tor as free software used to hide IP addresses from detection); *Tor: Overview*, *supra* note 44 (explaining that the more users Tor has, the more hidden each user can be).

49. *See* NPR Staff, *supra* note 42 (explaining that Tor is used by "human rights activists, journalists, military, law enforcement," political dissidents, and "normal people"). Indeed, due to its unique security, Tor saw a dramatic increase in its usage during the Arab Spring. *See id.* Additionally, because of its message of protecting civil liberties, Tor saw an increase after Edward Snowden's whistleblowing about the extent of the National Security Agency's (NSA) surveillance program. *See id.*

50. *See Jean*, 207 F. Supp. 3d at 925 (explaining that child pornography websites are frequently found in Tor's "hidden services" as its users feel anonymous).

To combat Tor's masking of IP addresses, the FBI "ran an end-around" and created a piece of software that would force a suspect's computer to reveal its IP address.[51] To combat Tor's masking of IP addresses, the FBI "ran an end-around" and created the NIT software, which is essentially malware, to force a suspect's computer to reveal its IP address.[52] Malware is an abbreviation for "malicious software" and is considered to be "any program or file that is harmful to a computer user."[53] These programs can be designed or coded to do anything from steal sensitive data to completely change the core functions of a computer.[54] Frequently, malware is designed to download to users' computers, without their knowledge or permission, after they have visited a malware-infected site.[55] Because of the negative connotation associated with the term malware, the FBI objected to the labeling of the NIT as such.[56] However, the term is the most apt description of the software used in *Lough*.[57]

B. *Search History: The Evolution of Fourth Amendment Search Analysis*

The United States Supreme Court has issued numerous opinions defining a "search" under the Fourth Amendment.[58] Perhaps no case has played a greater role in shaping this definition than *Katz v. United States*.[59] In *Katz*, the Court detailed a two-part reasonable expectation test for determining whether an

---

51. *See* United States v. Lough, 221 F. Supp. 3d 770, 773 (2016) (N.D. W. Va. 2016) (explaining that NIT software triggered suspect's computer to reveal IP address and other identifying information to FBI).

52. *See Jean*, 207 F. Supp. 3d at 927–28 ("The FBI was able to cause the user's computer to report the identifying information by exploiting a defective window in the TOR browser [sic], through which it ran what amounts to malware on the user's computer, with the objective being to override the TOR browser's and the user's computer security settings, and then 'cause' the user's computer to return discrete, content-neutral items of identifying information back to the FBI.").

53. *See* Margaret Rouse, *Malware (Malicious Software)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/malware [https://perma.cc/EP63-B6G8] (last visited Apr. 11, 2018) (providing basic definition of malware).

54. *See id.* ("These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission."). Examples of malware include viruses, Trojan horses, spyware, and Ransomware. *See id.*

55. *See id.* (describing the different methods of spreading malware; the method described here is called "drive-by download").

56. *See Jean*, 207 F.Supp.3d at 927 n.7 ("Agent Aflin objects to describing the NIT as malware, because the term has a derogatory connotation.").

57. *See Jean*, 207 F. Supp. 3d at 927 n.7 ("[W]hen used as a term of art to explain an ethical hacking technique used by law enforcement, the term malware is descriptive of the NIT used here."); *see also* United States v. Lough, 221 F.Supp.3d 770, 772-74 (describing the NIT used by the FBI).

58. *See supra* note 13 and accompanying text for examples of Supreme Court's Fourth Amendment jurisprudence.

59. 389 U.S. 347 (1967); *see* Fabio Arcila, Jr., *GPS Tracking out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 17 (2012) (stating that *Jones* is potentially the most important Fourth Amendment opinion since *Katz*, thereby recognizing *Katz* as most important Fourth Amendment case in forty years prior to *Jones*).

activity constituted a Fourth Amendment search.[60] Nevertheless, after decades of application, the Court reconsidered its early jurisprudence and modified the search analysis to include not only the *Katz* test, but also a test based on a physical intrusion by law enforcement.[61]

1. *The "Reasonable Expectation of Privacy" Test*

Prior to *Katz*, the governing rule regarding the Fourth Amendment stated that a search occurred only when a government agent physically intruded into a "constitutionally protected area."[62] The Court had made clear that "[w]hat a person knowingly exposes to the public . . . is not subject to Fourth Amendment protection."[63] This became an issue in *Katz*, where the FBI had been investigating the defendant for his participation in a gambling ring.[64] The FBI affixed a listening device to the outside of a public telephone booth to eavesdrop on the defendant's conversation.[65] Because the device never actually went inside the booth, the FBI's activity would not have constituted a Fourth Amendment search under the physical intrusion analysis.[66]

In shaping a new rule, the Court concluded in *Katz* that it did not matter where a search took place, but only whether a person expected that his or her information would not be made public.[67] Defined more clearly in Justice

60. *See Katz*, 389 U.S. at 353–59 (holding that the "trespass" doctrine for Fourth Amendment searches is no longer controlling and creating instead a test based on expectation of privacy).

61. *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("Fourth Amendment rights do not rise or fall with the *Katz* formulation."). Justice Scalia, writing for the Court, stated that the *Katz* test did not supplant the physical intrusion test, but merely supplemented it. *See id.* at 406–07.

62. *See Katz*, 389 U.S. at 351 (stating that "the Fourth Amendment protects people, not places"). The parties in *Katz* spent a large amount of their briefs debating whether a phone booth was a "constitutionally protected area." *See id.* Rather than examining where a particular search took place, the Court decided that when considering whether a search had occurred, the important factor to consider is whether an individual intended to expose that information to the public. *See id.*

63. *See id.* (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927)).

64. *See id.* at 348 (explaining that *Katz* was under investigation for "transmitting wagering information" using a public telephone booth).

65. *See id.* at 348 (explaining that device was used to listen to and record numerous calls by the defendant in order to obtain evidence of his criminal activity). The defendant used the phone to "transmit[] wagering information"; which meant he was caught illegally gambling using the phone booth. *See id.* Technically, the defendant's actions exposed him to the public. *See id.* Not only was the defendant using a public phone booth, but the booth was partially made of glass, therefore anyone walking past would see he made calls inside. *See id.* at 351. However, the Court stated that although he could be seen publicly, that when the door of the booth shut, it signaled the defendant's expectation that the conversation he had on the phone was meant to be private. *See id.* at 352–53.

66. *See id.* at 353 ("[T]he Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any 'technical trespass under . . . local property law.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))). "[T]he surveillance technique . . . employed involved no physical penetration of the telephone booth from which petitioner placed his calls." *Id.* at 352.

67. *See id.* at 352 ("One who occupies [a phone booth], shuts the door behind him, and

Harlan's concurrence, this new test featured two prongs.[68] The first prong of the test considers whether an individual had a subjective expectation of privacy.[69] The second prong of the test, the objective prong, asks whether this subjective expectation was one that society is willing to accept.[70] Therefore, an individual with a reasonable expectation of privacy cannot be subject to a warrantless or unreasonable search absent exigent circumstances.[71]

As the *Katz* test has been developed and applied over time, the Court has identified certain types of information that lack any reasonable expectation of privacy.[72] One such circumstance is the "third party doctrine."[73] Under this rule, any information conveyed to or shared with a third party loses any expectation of privacy it once had.[74]

Of particular importance to this area is the way in which the third party doctrine interacts with IP addresses.[75] Because an IP address is given to a user by an ISP, that information is, by necessity, shared with a third party.[76] Under

---

pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

68. *See id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement.").

69. *See id.* (stating that first a person must "have exhibited an actual (subjective) expectation of privacy").

70. *See id.* ("[S]econd . . . the expectation [must] be one that society is prepared to recognize as 'reasonable.'").

71. *See id.* at 357 (stating that searches conducted without a warrant are *per se* unreasonable "subject only to a few specifically established and well-delineated exceptions").

72. *See, e.g.*, United States v. Christie, 624 F.3d 558, 573–74 (citing "third party doctrine" and applying it to IP addresses); see, *e.g., Note, Everybody's Going Surfing: The Third Circuit Approves the Warrantless Use of Internet Tracking Devices in United States v. Stanley,* 56 B.C. L. REV. E-SUPPLEMENT 1, 5 (explaining that third party doctrine applies to dialed phone numbers, as customers voluntarily transmit that information to phone companies).

73. *See id.* at 574 (explaining "third party doctrine"); *see also* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[The Supreme Court] consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

74. *See Christie*, 624 F.3d at 573–74 (explaining that once information is "voluntarily conveyed" to a third party, a person "assume[s] the risk" that information will be provided to police); *see also* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) ("[B]y 'revealing his affairs to another,' an individual 'takes the risk . . . that the information will be conveyed by that person to the Government.'" (quoting United States v. Miller, 425 U.S. 435, 443 (1976))).

75. *See Christie*, 624 F.3d at 573–74 (discussing application of *Katz* reasonable expectation test to IP addresses). In *Christie*, the FBI obtained administrative control of a third party website offering illegal and obscene content. *See id.* at 563. Unlike in *Lough*, the site was not hidden with Tor, therefore the FBI simply took the list of IP addresses that had visited the site to the ISP and it matched the addresses with true identities. *See id. See also*, *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding third party doctrine applies and there is no expectation of privacy in IP address).

76. *See Christie*, 624 F.3d at 563 (explaining the process of assigning an IP address). IP addresses are assigned by an ISP every time the user connects to the internet. *See id.* "Depending on the ISP, a customer's IP address can change each time he logs on to the internet." *Id.* Website administrators also have access to a list of IP addresses that have visited their site, however they do not have access to the real names of the customers possessing each IP address. *See id.*

current law, an Internet user cannot have a reasonable expectation of privacy in an IP address because government agents can easily obtain that information from the ISP.[77]

2. *The "Common-law Trespassory" Test*

After over forty years of applying the *Katz* test, the Court shifted its viewpoint again in *Jones*, where it seemingly resurrected the idea that a Fourth Amendment search can also be tied to a "physical intrusion."[78] In *Jones*, the FBI attached a GPS device to a suspect's car and used it to track his movements.[79] The Court simplified the events of the case when it stated "[t]he Government physically occupied private property for the purpose of obtaining information," and that it had "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[80] Although the Court agreed that citizens have no reasonable expectation of privacy in their public locations, it reasoned that "the officers in this case did *more* than conduct a visual inspection of the defendant's vehicle."[81] By reviving the physical intrusion concept, the Court made clear that a full analysis for a Fourth Amendment search entails both the reasonable expectation of privacy test and the physical intrusion test.[82]

---

77. *See id.* at 574 ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."); *see also* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding that subscribers do not have subjective expectation of privacy in information conveyed to service providers because they "assumed the risk" that information could be handed over to police); United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (holding that information given to an ISP is not protected by Fourth Amendment).

78. *See* United States v. Jones, 565 U.S. 400, 408 (2012) (explaining that "*Katz* did not narrow the Fourth Amendment's scope," but merely supplemented original physical intrusion test).

79. *See id.* at 402–03 (explaining facts of the FBI investigation). From its position on "the undercarriage" of the vehicle, the device could establish "the vehicle's location within 50 to 100 feet." *See id.* at 403. It "communicated that location by cellular phone to a Government computer." *Id.* The FBI secured a warrant authorizing it to attach the device anywhere in the District of Columbia within ten days of securing the warrant. *See id.* at 402–03. However, the FBI attached the GPS on the eleventh day in the state of Maryland, violating the precise authorization of the warrant. *See id.* at 403. The district court "held the data admissible, because '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'" *See id.* at 403 (quoting United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006)).

80. *See id.* at 404–05 (explaining its holding that *Katz* test is mere supplement to original "common-law trespassory test"); *see also* New York v. Class, 475 U.S. 106, 111 (1986) (finding that even intrusion as slight as an officer reaching his arm into a vehicle is enough to constitute physical intrusion for Fourth Amendment purposes); *see also*, Thomas, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEX. TECH L. REV. 199, 206-215 (2010) (describing the colonial history that influenced the Framers' understanding of the Fourth Amendment).

81. *See Jones*, 565 U.S. at 410 (citation omitted) (distinguishing facts underlying *Jones* from those in *Class*).

82. *See id.* at 411 (making clear that full analysis is a combination of two tests rather than excluding one in favor of another). Justice Scalia, in response to criticism from the concurrence wrote that unlike those in favor of using only the *Katz* analysis, "we do not make

One obstacle facing the Supreme Court in reaching its conclusion in *Jones* was a pair of cases dealing with the use of "beepers" to track drug-making chemicals.[83] In *United States v. Knotts*,[84] the first of the two cases, law enforcement officials placed a beeper inside a drum containing a chemical precursor used to make illegal drugs.[85] The Court ruled that there was no reasonable expectation of privacy in public movements, so the fact that the beeper was placed in the drum without the purchaser's permission and used to follow the suspect's movements played no role in the analysis.[86]

In the second case, *United States v. Karo*,[87] the Court stated that until the beeper was used to monitor the suspect's location, there was no infringement of a privacy interest.[88] In a nearly identical set of facts to *Knotts*, the law enforcement officers in *Karo* placed a beeper into a drum used to store chemicals before it was sold to a suspected drug manufacturer.[89] While acknowledging that the installation of the beeper was a trespass, the Court in *Karo* ultimately held that it did not violate the Fourth Amendment.[90]

In the *Jones* opinion, Justice Scalia distinguished the installation of the devices in *Knotts* and *Karo* from the installation of the GPS tracker on the defendant's Jeep.[91] The notable difference in *Jones* was the fact that "the Government trespassorily inserted the information-gathering device," because

---

trespass the exclusive test." *See id.*

83. *See id.* at 409–10 (distinguishing ruling from those of *Knotts* and *Karo*).

84. 460 U.S. 276 (1983).

85. *See id.* at 277 (explaining that officers placed "beeper," or radio transmitter, inside of "five gallon drum containing chloroform purchased by" suspected drug manufacturer prior to delivery of the chemicals). Officers installed the beeper while the container was in the possession of the Hawkins Chemical Company. *See id.* at 278. The arrangement was such that when the defendant placed the next order, the company would make sure his product was placed in the drum containing the beeper. *See id.* Authorities used both the beeper as well as visual surveillance to track the container to a cabin. *See id.* at 278–79.

86. *See id.* at 281 (comparing privacy in location to the "diminished" privacy in a vehicle). "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* The Court also noted that it had "never equated police efficiency with unconstitutionality." *See id.* at 284. Essentially, the Court ruled that the beeper was just an extension of what was visible to the public; anyone watching the movements of the vehicle carrying the drum would have known the container was in the cabin. *See id.* at 285.

87. 468 U.S. 705 (1984).

88. *See id.* at 712 ("The mere transfer to Karo of a can containing an unmonitored beeper infringed no privacy interest. [The beeper] conveyed no information that Karo wished to keep private, for it conveyed no information at all.").

89. *See id.* at 708 (explaining that with consent from the chemical supplier, officers replaced can of ether, intended for delivery to defendant, with container of their own holding a beeper). Much like in *Knotts*, the government used the beeper to track the movements of the can and eventually led to subsequent searches and arrests. *See id.* at 708–10.

90. *See id.* at 712–13 ("At most, there was a technical trespass on the space occupied by the beeper. The existence of a physical trespass is only marginally relevant to the question of whether the Fourth Amendment has been violated . . . ."). The *Karo* court established that the mere act of transferring to *Karo* a container with a beeper was not a Fourth Amendment search. *See id.* at 712. It was not until the authorities began monitoring the beeper that a potential for a violation was possible. *See id.*

91. *See* United States v. Jones, 565 U.S. 400, 408–10 (2012) (summarizing holdings in *Knotts* and *Karo*).

the vehicle was in the defendant's possession at the time of the installation.[92] In *Knotts* and *Karo*, however, the installation occurred before the containers were in the defendant's possession.[93] Therefore, the seemingly inconsistent conclusions between *Jones* and the two prior cases are reconcilable under the physical intrusion test.[94]

C. *Get off my Cyberlawn: Is Cybertrespass a Thing?*

An emerging issue that plays a substantially important role in the discussion of the NIT as a Fourth Amendment search is whether someone can trespass in cyberspace, and many courts have held the digital transmission of unwanted signals is enough to establish a trespass.[95] Nevertheless, one commenter finds it troubling for courts to be establishing the tort of cybertrespass, worrying that it will stunt the free growth of the Internet.[96] Yet, another legal commenter argues that advances in cybertrespass law are beneficial because advancements allow companies to protect their investments in web-resources.[97]

Although Congress has not created a statute specifically defining the crime of cybertrespass, it has criminalized the act of interfering with "protected

92. *See id.* (explaining that the difference lies in the time period of installation of tracking devices).

93. *See id.* at 409 (explaining that in both cases a device was placed into container while it was still in possession of the respective chemical distributor).

94. *See id.* at 410 (holding that because the Jeep was in defendant's possession at the time the GPS was attached, FBI had physically intruded into his property). Whereas in *Knotts* and *Karo*, the government could not have intruded into defendants' property as drums were not in possession of defendants when devices were attached. *See id.*

95. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000) (holding that electronic signals are tangible enough to establish trespass action); America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (holding that even without physical damage to the computer, unwanted spam was still a trespass); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (recognizing a viable claim for trespass where defendant sent unwanted electronic signals to plaintiff's network); Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996) (holding that it is a trespass to "hack" into a computer system to make free long distance telephone calls); Washington v. Riley, 846 P.2d 1365, 1373 (Wash. 1993) (en banc) ("[A] person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another." (quoting WASH. REV. CODE § 9A.52.110 (repealed 2016))).

96. *See* Edward W. Chang, *Bidding on Trespass:* eBay, Inc. v. Bidder's Edge, Inc. *and the Abuse of Trespass Theory in Cyberspace-Law*, 29 AIPLA Q.J. 445, 446 (2001) (arguing that unbridled expansion of cybertrespass law is dangerous). Chang was particularly concerned with the idea that in *eBay*, the court allowed for minimal damage or use to be sufficient to support an action for trespass. *See id.* at 462–64; *see also eBay, Inc.*, 100 F. Supp. 2d at 1071 (holding that even though the defendant used a very small percentage of plaintiff's resources, it still committed actionable trespass).

97. *See generally* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73 (2003) (advocating for an even more liberal set of cybertrespass laws). Epstein states that he believes cybertrespass should develop to mirror the law of real property. *See id.* at 82–83. His reasoning is that cyber entities are "fixed" in their cyber locations just as real property is fixed to its position on land. *See id.* at 83. This would mean that plaintiffs would not be required to show any real damage at all in order to state a sufficient cybertrespass claim. *See id.* at 78.

computers" through the Computer Fraud and Abuse Act (CFAA).[98] Under the CFAA, it is illegal to access a computer for the purpose of obtaining information without permission.[99] While the CFAA has been criticized for being overly broad, it sends a signal to courts that Congress considers unauthorized computer access to be a serious offense.[100]

III. DOWNLOAD COMPLETE: THE FBI'S PLAYPEN STING

The *Lough* case, and its many companions, stem from a common nucleus of facts surrounding an FBI sting of a child pornography website.[101] In December 2014, the FBI learned that a child pornography website was operating on the Tor network under the name "Playpen."[102] Due to the masking process of the Tor software, the FBI struggled to locate the server running the website.[103] However, on February 20, 2015, the FBI was able to seize the server hosting Playpen from a web-hosting facility in North Carolina.[104] Rather than disabling Playpen and permanently removing it from the Dark Web, the FBI continued operating the website for thirteen days.[105]

The seizure of Playpen and the arrest of its owner allowed the FBI to assume administrative control over the website.[106] Even though FBI agents

98. 18 U.S.C. § 1030 (2012) (criminalizing certain uses of computers by government and in interstate commerce).

99. *See id.* § 1030(a)(2)(c) ("[It is a crime to] intentionally access a computer without authorization or [when authorization is exceeded], and thereby obtain[] . . . information from any protected computer").

100. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1568 (2010) (examining the criticisms of the definition of "protected computer"). Under the act any computer in interstate commerce is "protected" and in reality every computer is engaged in interstate commerce. *See id.*

101. *See* United States v. Lough, 221 F. Supp. 3d 770, 772 (N.D. W. Va. 2016) (explaining that Playpen was used as a means for unsavory individuals to look at, share, and download child pornography).

102. *See id.* (explaining that Playpen was operated in secrecy of the Tor network where users could hide from law enforcement by masking their true identities and IP addresses). In order to access Playpen, users needed to sign in using a username and password. *See id.* at 773. The site had approximately 215,000 members, of which the NIT was deployed against 1,300. *See* Nakashima, *supra* note 1 (discussing Playpen sting and government's use of malware to identify child pornography offenders).

103. *See* United States v. Jean, 207 F. Supp. 3d 920, 925–26 (W.D. Ark. 2016) (explaining that, due to complete anonymity of Tor network, there was no way for the FBI to identify or locate site's operator).

104. *See id.* at 925 ("[T]he FBI received a serendipitous break [in its search for the Playpen owner]."). While the site was going through an update, the owner of the site mistakenly deactivated the Tor cloaking settings. *See id.* This left the Playpen site exposed for "a few days." *See id.* The deactivated settings opened a window wide enough for the FBI to find the server that was hosting Playpen. *See id.* After seizing the server, the FBI arrested the site's owner on February 19, 2015. *See id.*

105. *See id.* at 926; *see also Lough*, 221 F. Supp. 3d at 773 (explaining that FBI continued to administer site in order to identify users who were involved with abuse of children). Playpen was kept open from February 20, 2015 until March 4, 2015. *See Jean*, 207 F. Supp. 3d at 926. To accomplish this task, "agents made a copy of the Playpen website," placed it on a government server, and assumed administrative control over it. *See id.*

106. *See Jean*, 207 F. Supp. 3d at 925–26 (restating the process by which FBI gained control of Playpen).

working the case became the administrators of the website, due to the Tor network they had no way of identifying visitors.[107] In order to solve the dilemma, the FBI created a piece of software, the NIT, and obtained a federal warrant to deploy it.[108]

The NIT was deployed when a website visitor "clicked on a forum link to begin downloading child pornography."[109] The NIT would then "surreptitiously deploy" and force the "activating computer" to send certain identifying information to the FBI.[110] In addition to the computer's IP address, the NIT relayed to the FBI the type of operating system used by the computer, the computer's "Host Name," and the computer's media access control (MAC) address.[111]

The defendant in *Lough* was one of many to have accessed Playpen while it was under the FBI's control.[112] His IP address was revealed when the FBI deployed the NIT against his computer.[113] To obtain the defendant's actual identification, the FBI subpoenaed his ISP.[114] Using the information from the NIT and the ISP, the FBI obtained a search warrant authorizing agents to search

---

107. *See id.* at 926 ("The users' identifying information was purposely unknown to Playpen's owner, and the users' IP addresses remained concealed because the website was only accessible as a hidden service on the TOR network, thus providing total anonymity to the users.").

108. *See Lough*, 221 F. Supp. 3d at 772–73 (describing the process used by the FBI to obtain a NIT warrant). For the purposes of this Note, the fact that the FBI actually obtained a warrant makes no difference; the *Lough* court concluded that one was not needed because the NIT was not a Fourth Amendment search. *See id.* at 775–76. The judge that issued the warrant was a federal magistrate judge from the Eastern District of Virginia. *See id.* at 776; *Jean*, 207 F. Supp. 3d at 926. Much of the controversy regarding the warrant stems from the fact that it applied to "searches" across the country and outside the jurisdiction of the magistrate judge. *See* Nakashima, *supra* note 1. An attorney representing a defendant similar to Lough, stated, "There has never been any warrant . . . that allows searches on that scale. It is unprecedented." *See id.*

109. *See Jean*, 207 F. Supp. 3d at 927 (explaining that to deploy the NIT numerous affirmative actions were necessary, including logging into the Playpen website using a username and password and clicking on forum to begin download). The NIT and the illegal content would download simultaneously. *See id.* at 928.

110. *See id.* at 928 (explaining that entire process of transmitting information occurred before child pornography had even completed its download). The NIT worked "by exploiting a defective window in the TOR browser, through which it ran what amounts to malware on the user's computer." *Id.* at 927 (footnote omitted). This process is what forced the computer to return information to the FBI. *See id.* at 928.

111. *See id.* at 926 (stating that although this information allowed the FBI to obtain identifying information about suspect's computer, they were not given any information about the suspects "true identity" in physical world). For efficiency purposes the NIT also generated a "unique identifier" each time it was deployed and kept track of whether or not the NIT had been previously deployed on the particular "activating computer." *See id.*

112. *See* Nakashima, *supra* note 1 (stating that over 130 persons have been charged in relation to Playpen sting).

113. *See Lough*, 221 F. Supp. 3d at 773 ("Utilizing the NIT, the FBI determined that a user living in Fairmont, West Virginia, with the username '2tots,' had logged into the Playpen website and accessed child pornography.").

114. *See id.* ("An administrative subpoena served on Frontier Communications Corporation [the ISP] established that the IP address for '2tots' belonged to Lough's account, which was registered to a street address later determined to belong to him.").

the defendant's home.[115] On March 23, 2016, the defendant pled guilty to child pornography charges but later moved to withdraw the plea.[116] In September 2016, the defendant moved to suppress all evidence that resulted from the NIT warrant.[117] After carefully considering the arguments presented by the parties, the court concluded that a discussion of the warrant was not necessary to the court's determination because the NIT did not constitute a search under the Fourth Amendment.[118]

IV. NO HIDING BEHIND A KEYBOARD: THE *LOUGH* COURT CONCLUDES IP ADDRESS IS PUBLIC INFORMATION

To determine whether the evidence stemming from the NIT should be suppressed, the *Lough* court first had to determine whether the NIT constituted a search under the Fourth Amendment.[119] In analyzing this question, the court

115. *See id.* (stating that the FBI secured a warrant to raid the suspect's home and that after the raid, agents seized "multiple pieces of evidence suspected of containing child pornography").

116. *See id.* (recounting that Lough waived his right of indictment, "acknowledged the facts" presented by the FBI agent, and admitted to charges). On May 4, 2016, Lough moved to withdraw the plea after learning of another court that had suppressed evidence stemming from the NIT. *See id.*

117. *See id.* (explaining rationale for Lough's motion). Lough argued that the evidence must be excluded because the warrant was invalid. *See id.* The government argued that the warrant was valid as the NIT acted as a tracking device. *See id.* Magistrate judges are allowed to authorize the installation of a tracking device in their own district, even if the subject then leaves the district of installation. *See* FED. R. CRIM. P. 41(b)(4) ("[A] magistrate judge . . . has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both[.]"). Many courts, including *Lough* and some of its companions, have concluded that Rule 41(b)(4) gave the magistrate judge in Virginia the power to authorize the NIT warrant, even though the IP address would be transmitted from states outside the magistrate's jurisdiction. *See, e.g.*, *Lough*, 221 F. Supp. 3d at 777 ("[B]ecause the NIT is analogous to a tracking device in both function and effect, the magistrate judge was authorized under Rule 41(b)(4) to issue a warrant for its use."); *see also* United States v. Jean, 207 F. Supp. 3d 920, 937–38 (W.D. Ark. 2016) (holding that because NIT "was an electronic tool or technique designed and executed for the purpose of tracking the movement of information" warrant was authorized under Rule 41(b)(4)); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *7 (C.D. Cal. Aug. 8, 2016) ("The fact that courts are presently divided over whether the NIT Warrant even violated Rule 41 is compelling evidence that the FBI did not intentionally and deliberately violate that Rule by seeking the warrant in the first instance."); United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016) (holding that because "[u]sers of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site" NIT acted as a tracking device and is authorized under Rule 41(b)(4)); United States v. Eure, No. 2:16cr43, 2016 WL 4059663, at *9 (E.D. Va. July 28, 2016) ("Even if the FBI agents had some indication that the warrant might exceed the jurisdiction of the magistrate judge, there were credible arguments that the current rule allowed this warrant."). *But see* United States v. Weredene, 188 F. Supp. 3d 431, 447 (E.D. Pa. 2016) (concluding that NIT software was "attached" in defendant's state which was outside of magistrate's jurisdiction, but that error was too minor to require suppression).

118. *See Lough*, 221 F. Supp. 3d. at 782–83 (concluding that defendant had no reasonable expectation in IP address so warrant was unnecessary, but also concluding that the warrant was valid even if required).

119. *See id.* at 774 ("The initial question presented here is whether Lough had the kind

solely applied the *Katz* reasonable expectation test.[120] As mentioned above, the *Katz* test requires that the individual has a subjective expectation of privacy *and* that the subjective expectation be one that society is prepared to accept.[121] Specifically, the court stated that, for the defendant's suppression motion to be granted, he must have demonstrated a reasonable expectation of privacy in the IP address sent to the FBI by the NIT.[122]

Under the first subjective prong of the *Katz* test, the court determined that the defendant could not have had a subjective expectation of privacy due to the third party doctrine.[123] The court noted that while the defendant wished to remain anonymous using the Tor network, hoping to remain anonymous is not equal to expecting it.[124] Because the IP address had been communicated to numerous computers in the Tor chain, Lough could not have had a subjective expectation of privacy in the IP address.[125]

After the defendant did not satisfy the first prong of the *Katz* test, the analysis could have concluded.[126] However, the court went on to explain that even if Lough had demonstrated a legitimate subjective expectation, he would not have passed the objective prong of the *Katz* test.[127] The court noted that every federal court that has discussed the issue of privacy in IP addresses has

---

of reasonable expectation of privacy in his IP address that society is prepared to recognize."). The court also discussed whether the specific warrant authorizing the NIT was sufficient to conduct a search. *See id.* at 774–75. In its opinion, the court also noted that "the vast majority of courts addressing [this] issue have found suppression unwarranted." *See id.* at 774.

120. *See id.* at 775 (stating the requirement for a defendant to demonstrate a reasonable expectation of privacy). Although the *Lough* court does not cite directly to *Katz*, it is clear that they were applying the test. *See id.* (explaining the need for both a subjective and objective expectation of privacy).

121. *See id.* (explaining that defendant did not have a reasonable expectation of privacy in an IP address and refraining from analyzing whether society would recognize this expectation of privacy). The court also defined "objectively reasonable" to mean one "'that society is willing to recognize as reasonable.'" *See id.* (citing United States v. Castellanos, 716 F.3d 828, 832 (4th Cir. 2013)); *see also* Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring) (enunciating two prongs of the reasonable expectation test). For a further discussion of *Katz*, see *supra* notes 62-77 and accompanying text.

122. *See Lough*, 221 F. Supp. 3d at 775 ("Absent a legitimate expectation of privacy, Lough cannot invoke the protections of the Fourth Amendment."). The court concluded that Lough cannot meet this expectation test for his IP address. *See id.*

123. *See id.* ("Lough could not have had a subjective expectation of privacy because he voluntarily turned over his IP address to every computer with which he made contact, including the first node of the TOR network.").

124. *See id.* (stating explicitly that, although the defendant "hoped that the TOR would facilitate" anonymity, "hoping and wishing are not the equivalent of expecting a certain result"). The court stated, "At the very least, Lough certainly knew that he was revealing his IP address to one unknown third party who, for all he knew, was a law enforcement officer." *Id.* (footnote omitted).

125. *See id.* (holding that because Lough had revealed "his affairs to another he t[ook] the risk that" the "information will be conveyed by that person to the Government") (quoting United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016)).

126. *See Katz*, 389 U.S. at 361–62 (explaining that subjective expectation must be established first and if one does not exist then the analysis ends there).

127. *See Lough*, 221 F. Supp. 3d at 775 ("Even assuming that Lough did have a subjective expectation of privacy, it is not one that society is prepared to recognize as reasonable." (citation omitted)).

concluded there is no objective expectation of privacy in them.[128]

The *Lough* court recognized that individuals certainly have a privacy interest in items inside their homes, such as their computer and its contents.[129] However, the court distinguished Lough's privacy interest in his computer and its contents from his lack of a privacy interest in his computer's IP address.[130] Thus, the court determined that because the computer's contents were not searched by the NIT, there was no Fourth Amendment search with respect to the defendant's computer.[131] Having concluded that neither the IP address nor other information gathered by the NIT constituted a search, the court denied Lough's motion to suppress the evidence stemming from the NIT.[132]

By determining that there was no Fourth Amendment search, the court ruled that no warrant was necessary to utilize the NIT.[133] Nevertheless, the court examined the validity of the warrant authorizing the NIT.[134] The court determined that because the NIT was, for all intents and purposes, a tracking device, the issuing magistrate had authority to supply the FBI with the warrant used to implement the NIT.[135] In coming to its conclusion, the court analogized the way users visited the Playpen website to physically traveling to the location of the FBI-run server, where agents then virtually attached the tracking

---

128. *See id.* at 775–76 (citing United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)).

> Even if the defendant could show that he had a subjective expectation of privacy in his subscriber information, such an expectation would not be objectively reasonable. Indeed, "every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."

Bynum, 604 F.3d at 164 (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008)).

129. *See Lough*, 221 F. Supp. 3d at 776 ("Clearly, Lough does have a privacy interest in his home and its contents, including his computer.").

130. *See id.* (distinguishing between the search of the contents of the defendant's computer and the FBI's use of the NIT to identify the IP address of defendant's computer and concluding that the former gave rise to a privacy interest while latter did not).

131. *See id.* (citing United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016)) (noting clear distinction made between content-based communications and non-content information and concluding that the NIT did not conduct search of contents of defendant's computer).

132. *See id.* at 783 ("Lough had no reasonable expectation of privacy in his IP address, nor did the NIT constitute a Fourth Amendment search of the content of his computer; thus, a warrant was unnecessary; . . . Accordingly, the Court denies Lough's motion to suppress.").

133. *See id.* (determining that warrant was unnecessary where defendant had no reasonable expectation of privacy in IP address and where there was no search of defendant's computer).

134. *See id.* at 776–78 (analyzing validity of warrant and explaining the defendant's contention was that the warrant exceeded the scope of the issuing magistrate's authority, but concluding that the nature of NIT allowed the magistrate to have authorized its use).

135. *See id.* at 777 ("Nevertheless, because the NIT is analogous to a tracking device in both function and effect, the magistrate judge was authorized under Rule 41(b)(4) to issue a warrant for its use."). The court also noted that the companion case of *Jean* "tallied the courts that have specifically addressed whether the NIT was akin to a tracking device." *See id.* Many of the tallied courts have used the analogy of a "virtual trip" to determine the NIT is the functional equivalent of a tracking device. *See id.*

device—the NIT—to a user's "vehicle."[136] Thus, the NIT was a tracking device authorized by a legal warrant.[137]

V. ERROR, INCOMPLETE DISC: COMPLETING THE FOURTH AMENDMENT SEARCH ANALYSIS

While many courts have come to similar conclusions regarding the NIT—and these conclusions may not necessarily be incorrect—the *Lough* court did not complete the Fourth Amendment search analysis prescribed in *Jones*.[138] The full determination of a search should have included both the *Katz* reasonableness test and the *Jones* physical intrusion test.[139] Had the *Lough* court completed this analysis, it very well may have come to the conclusion that the NIT was in fact a search protected by the Fourth Amendment.[140] Additionally, companion cases suggest that the issue of whether there is a reasonable expectation of privacy in IP addresses could have been decided in favor of the defendant in *Lough*.[141] If examined under both the *Katz* and *Jones*

---

136. *See id.* at 778 (agreeing with and following other courts' "virtual trip" analogy). The court stated:

> Lough took a virtual trip to the Eastern District of Virginia, but rather than travel by car, he traveled digitally—his vehicle was comprised of packets of information. Once there, the FBI attached a digital electronic tracking device to those packets, which Lough virtually rode back to the Northern District of West Virginia. Upon his virtual return, Lough parked his digital vehicle built of those packets of information on his computer, rather than in his driveway. At that point, the NIT sent back his digital address, just as a GPS tracker would send back his coordinates.

Id.

137. *See id.* ("Accordingly, the NIT is analogous to a tracking device . . . and the NIT warrant is an information-tracking warrant that comports with [the law], which [the magistrate] had the authority to issue.").

138. *See id.* at 775 (holding that because Lough had no reasonable expectation of privacy in information taken by the malware, NIT was not a search); United States v. Jean, 207 F. Supp. 3d 920, 933 (W.D. Ark. 2016) ("[T]he FBI in the instant case was under no legal obligation to obtain a search warrant . . . as IP addresses are unlikely to be entitled to the same Fourth Amendment protections as are the substantive contents of users' computers."); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016) (proclaiming that NIT was not a search); United States v. Eure, No. 2:16cr43, 2016 WL 4059663, at *9 (E.D. Va. July 28, 2016) (holding that "searches and seizures perform[ed] pursuant to the NIT did not violate Fourth Amendment"); United States v. Weredene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016) (holding that Weredene's computer was not searched because he had no reasonable expectation of privacy in his IP address).

139. *See* United States v. Jones, 565 U.S. 400, 406 (2012) (explaining that the *Katz* test does not supersede the "physical intrusion" test, rather it supplemented it). The Court stated, "Fourth Amendment rights do not rise or fall with the *Katz* formulation." *Id.*

140. *See* United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) (holding that NIT is search because "government literally . . . invaded the contents of the computer"); *see also* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016) (holding NIT was "unquestionably a 'search' for Fourth Amendment purposes" because it "placed code on [the] computer without [the defendant's] permission"). Although these two *Lough* companion cases do not explicitly analyze the situation under the *Jones* test, both seem to use the idea of a physical intrusion to label the NIT a search. *See Torres*, 2016 WL 4821223, at *3; *Darby*, 190 F. Supp. 3d at 530.

141. *See, e.g.*, United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016) (holding that there is a reasonable expectation of privacy and that the third party doctrine does

tests, the NIT should be considered a search under the Fourth Amendment.[142]

A. *The NIT Is a Search Under the Katz Test*

While the majority of courts have determined that IP addresses are subject to the third party doctrine, there is evidence that the third party doctrine may not apply to the specific facts of *Lough*.[143] Indeed, at least one court challenges this idea by distinguishing between the government's retrieval of information directly from the defendant using surveillance or an invasive technique and the government's retrieval of the information from some business or other third party.[144] For example, when the government obtains records from a business via subpoena, there is an inherent decrease, or even elimination, of the privacy interest.[145] Thus, if under *Katz* the defendant's reasonable expectation of privacy depends on how the government retrieved the information at issue, then it follows that information retrieved from a third party loses the expectation of privacy, whereas information retrieved using an invasive technique does not.[146]

The *Lough* court concluded that the FBI's use of the NIT fell within the third party doctrine of the Fourth Amendment because the defendant had provided his IP address to both his ISP and to other nodes on the Tor network.[147] However, the NIT pulled the IP address and related information directly from the suspect's computer.[148] The FBI did not gain access to this

---

not apply here because the FBI did not obtain IP address from third party but from computer itself).

142. *See id.* (applying *Katz* and finding NIT to be Fourth Amendment search); *see also Darby*, 190 F. Supp. 3d at 528, 530 (finding a Fourth Amendment search due to apparent government intrusion in the context of a *Jones* discussion).

143. *Cf.* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("Whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it."). In *Carpenter*, the court noted a distinction between police accidentally overhearing a phone conversation in a public place (not protected by the Fourth Amendment) and using a wiretap to hear that same conversation (protected by the Fourth Amendment). *See id.*

144. *See id.* at 889 (highlighting two ends of the Fourth Amendment spectrum and noting that information collected from third parties is on one end and is unprotected by the Fourth Amendment, while information retrieved by government from suspect via some surveillance or other invasive technique is on the other end).

145. *See id.* ("[B]usiness records obtained from a third party . . . can only diminish the defendants' privacy in the information those records contain." (citations omitted)).

146. *See id.* at 888–89 (distinguishing *Jones* from *Carpenter* and concluding that, while there was reasonable expectation of privacy in *Jones*, there was no such expectation in *Carpenter*). The court stated, "[T]he government action in this case is very different from the government action in *Jones*. That distinction matters: in applying *Katz*, 'it is important to begin by specifying *precisely the nature of the state activity that is challenged*.'" *Id.* at 888 (emphasis in original).

147. *See* United States v. Lough, 221 F. Supp. 3d 770, 775 (N.D. W. Va. 2016) (explaining that the third party doctrine applies to those who expose their information to others and assume risk that this information may be turned over to government and finding it applied here because Lough gave his IP address to every computer with which he made contact).

148. *See* United States v. Jean, 207 F. Supp. 3d 920, 926 (W.D. Ark. 2016) (describing that NIT deployed secretly on "activating computer" and sent information directly to FBI).

information by subpoenaing the ISP or the other Tor users.[149] Indeed, the point of using the NIT was to obtain the IP addresses without going to some source other than the suspects themselves; moreover, the FBI could not have retrieved the IP addresses from any third party because the third party would not have been able to undo the camouflage created by Tor.[150]

Even one of *Lough*'s companion cases, decided a few months earlier, concluded that defendants subjected to the NIT had a reasonable expectation of privacy in their IP addresses and computers.[151] While conceding that individuals generally have no expectation of privacy in their IP addresses, the companion court noted that the FBI obtained the IP address from the defendant's personal computer rather than from an ISP.[152] The real question, according to the companion court, was whether defendants have a reasonable expectation of privacy in their private computers.[153] Generally, courts have concluded that they clearly do.[154] Through this lens, the companion court concluded that implementing the NIT and forcing code upon the defendant's computer violated a reasonable expectation of privacy; thus, under the *Katz* test alone, the NIT was a search for purposes of the Fourth Amendment.[155]

Even if the companion court's conclusion was incorrect, at least one Supreme Court Justice has recently called for an evolution of Fourth Amendment jurisprudence to correspond with the new digital age.[156] In her concurrence in *Jones*, Justice Sotomayor acknowledged that America's search and seizure jurisprudence is outdated and that people's expectations of privacy

149. *See id.* (explaining that "[t]he users' identifying information was purposely unknown to Playpen's owner, and the users' IP addresses remained concealed because the website was only accessible as a hidden service on the TOR network," thus, the FBI could not have gone to an ISP to get the IP addresses as they had no way of knowing who they were targeting).

150. *See Lough*, 221 F. Supp. 3d at 772–73 (stating the FBI created the NIT for the purpose of obtaining information about those persons accessing the website).

151. *See* United States v. Ammons, 207 F. Supp. 3d 732, 739 (W.D. Ky. 2016) ("There appears to be no dispute that Ammons enjoyed a subjective expectation of privacy in the contents of his personal computer. His expectation was reasonable too." (citation omitted)).

152. *See id.* (noting that warrant listed the defendant's computer as things to be searched). The *Ammons* court appears to change the analysis from examining the IP address to examining the expectation defendants have in their computers. *See id.* By reframing the issue, the court easily determined that the third party doctrine did not apply because the defendant did not share his computer with a service provider—he only shared his IP address—and the NIT searched his computer. *See id.*

153. *See id.* ("The Government elides the fact that the NIT warrant describes Ammons' computer as the thing to be searched . . . . Accordingly, the pertinent inquiry is whether Ammons had a reasonable expectation of privacy in the contents of his personal computer—not merely in his IP address." (citations omitted)).

154. *See id.* ("Generally speaking, computer users have a reasonable expectation of privacy in data stored on a home computer." (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001))).

155. *See id.* (concluding that the NIT was a search under the *Katz* test because it intruded on the defendant's reasonable expectation of privacy); *see also* United States v. Darby, 190 F. Supp. 3d 520, 529–30 (E.D. Va. 2016) (holding that placing code on a defendant's computer constituted search).

156. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

have likely changed over time.[157] Justice Sotomayor advocated for decoupling secrecy and privacy when it comes to the Fourth Amendment.[158] Just because something is publicly available does not mean society would be willing to accept that there is no privacy interest in it.[159] Unfortunately for the defendants whose IP addresses are obtained via NIT , such an evolution of the law has not occurred to date, and the *Lough* court's interpretation of *Katz* appears to be the prevailing view.[160]

B. *The NIT Is a Search Under the Jones Test*

Even while giving deference to the *Lough* court's conclusion with regard to the *Katz* test, it is still possible to conclude that the NIT was search.[161] Although none of *Lough*'s companion cases explicitly cite to *Jones*, their reasoning indicates that the idea of a physical intrusion played a role in their decisions.[162] Despite the fact that the Supreme Court's decision in *Jones* incorporated the physical intrusion test into any Fourth Amendment search analysis, the *Lough* court relied solely on the *Katz* test.[163]

The *Lough* court should have inquired whether the NIT constituted a physical intrusion of the defendant's computer.[164] Interestingly, the court

---

157. *See id.* at 417–18 (noting "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" and "doubt[ing] that people would accept without complaint the warrantless disclosure to the Government of a list of every web site they had visited in the last week, or month, or year.").

158. *See id.* at 418 ("[W]hatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.").

159. *See id.* ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." (citation omitted)).

160. *See* United States v. Lough, 221 F. Supp. 3d 770, 774-76 (N.D. W. Va. 2016) (noting that the opinion is guided by "the vast majority of courts" that have addressed similar issues and found suppression of NIT evidence unwarranted).

161. *See* United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) (noting that the placement of code on the defendant's computer constitutes a government intrusion and thus, a Fourth Amendment search). The *Darby* court also noted that it is irrelevant that some of the information seized lacked a reasonable expectation of privacy. *See id.*

162. *See id.* ("In placing code on Defendant's computer, the government literally . . . invaded the contents of the computer. Additionally, the code . . . caused Defendant's computer to transmit certain information without the authority or knowledge of Defendant."); *see also* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016) ("[T]he NIT placed code on [the] computer without [defendant's] permission . . . [thus, the NIT] was unquestionably a 'search' for Fourth Amendment purposes.").

163. *See Lough*, 221 F. Supp. 3d 775–76 (analyzing a Fourth Amendment search using only a reasonable expectation of privacy test and without any discussion of whether the NIT was a physical intrusion); *see also Jones*, 565 U.S. at 407 (majority opinion) ("*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))).

164. *See Jones*, 565 U.S. at 404 (holding that physical intrusions are considered searches for the purposes of the Fourth Amendment). In *Jones*, the installation and use of GPS was deemed a search because "[t]he Government physically occupied private property

displayed this type of reasoning when it described the NIT as a tracking device and used the "virtual trip" analogy.[165] In analogizing the installation and use of the NIT to that of a GPS tracker, the court should have realized the factual similarities to *Jones*, as well as *Knotts* and *Karo*.[166] In these cases, as well as in *Lough*, the government affixed a device for the purpose of obtaining information.[167] While this action did not constitute a search in *Knotts* and *Karo*, it did in *Jones*.[168]

Importantly, the facts of *Lough* are more similar to *Jones* than to *Knotts* and *Karo*.[169] In *Lough*, the NIT was virtually placed on the defendant's computer without his knowledge or consent, and the computer was inside of his home when this occurred.[170] Unlike the facts in *Knotts* and *Karo*, Lough's computer was in his possession when the government affixed its "tracking device" to it.[171] Companion cases of *Lough* indicated that the FBI's placement of malware onto a computer without the owner's permission equates to a physical intrusion, even if they do not explicitly state that conclusion.[172]

---

for the purpose of obtaining information." *See id.*

165. *See Lough*, 221 F. Supp. 3d at 778 (comparing the NIT to a GPS tracker). The court in *Lough* likened the defendant's visit to Playpen to him taking a trip via car. *See id.* Much like in *Jones*, where the FBI attached a GPS to a defendant's Jeep, in *Lough* the FBI attached the NIT to the defendant's virtual vehicle. *See id.*; *see also Jones*, 565 U.S. at 403. The *Lough* court analogized the transmission of the IP address to the transmission of location data from a GPS. *See Lough*, 221 F. Supp. 3d at 778. Thus, the court concluded, the NIT was akin to a GPS tracker. *See id.*

166. *See Jones*, 565 U.S. at 403 (stating that police affixed a GPS tracker to the defendant's vehicle and that this practice constituted a search under the Fourth Amendment); *see also* United States v. Karo, 468 U.S. 705, 708 (1984) (explaining that in order to track movements of suspected drug manufacturer, police obtained permission from the chemical distributor to swap a drum of ether with a drum bugged with a beeper); *Knotts*, 460 U.S. at 278–79 (1983) (explaining that law enforcement officials placed a radio transmitter inside of a chemical drum, while in possession of the chemical distributor, in order to track the movements of suspected drug manufacturers).

167. *See Karo*, 468 U.S. at 712 (describing the installation of a beeper inside the can of ether); *Knotts*, 460 U.S. at 278 (describing installation of beeper inside five-gallon container of chloroform).

168. *See Jones*, 565 U.S. at 409–10 (differentiating itself from *Knotts* and *Karo* due to the fact that in the beeper cases, potential intrusions occurred before property was held by defendants, while in *Jones* the vehicle the government bugged was owned and in possession of the defendant); *see also Karo*, 468 U.S. at 712 (holding that beeper's placement did not infringe a privacy interest); *Knotts*, 460 U.S. at 281 (holding that the act of installing a beeper into a vat of chemicals is not in itself a search).

169. *See Lough*, 221 F. Supp. 3d at 773 (describing the process used by the NIT to transfer the data); *see also Jones*, 565 U.S. at 409–10 (differentiating itself from *Knotts* and *Karo* because the government bugged item that was owned and in possession of the defendant).

170. *See id.* at 773, 778 (explaining that the NIT was transmitted from FBI headquarters directly onto defendant's computer and that under the court's "virtual trip" analogy neither defendant nor his computer actually left his home in West Virginia).

171. *See id*. at 778 (stating defendant's computer never left his house, thus creating "virtual trip" analogy); *see Karo*, 468 U.S. at 708 (explaining that the beeper was placed into a container belonging to law enforcement who then swapped it with one set to be purchased by defendant); *Knotts*, 460 U.S. at 278 (stating that the beeper was installed while the container was in possession of the chemical company).

172. *See* United States v. Darby, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016) (noting that

Perhaps the reason courts have been reluctant to apply the physical intrusion test to the NIT is the fact that the intrusion occurred digitally.[173] Yet, in *Jones*, Justice Scalia noted that the intrusion test has always been tied to the law of trespass.[174] Although the Supreme Court may be slow to react when it comes to technology, numerous courts have expanded trespass into the cyber realm.[175]

Electronic signals appear to be enough to establish a cybertrespass, and the threshold requirement of damage or occupation is minimal.[176] The concept of Cybertrespass suggests that the FBI physically intrudes into a defendant's computer by sending an unwanted signal occupying a small portion of a defendant's hard drive space.[177] As it applies to *Lough*, by combining the notions that a cybertrespass requires a very small amount of storage to be occupied and that a physical intrusion can be as minimal as an officer reaching into a vehicle, it can be argued that the implementation of the NIT without the computer owner's permission would constitute a Fourth Amendment search.[178]

---

the government literally intruded into defendant's computer by placing code there without permission); *see also* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016) (holding that by installing the NIT without permission, the government "unquestionably" committed Fourth Amendment search and seizure).

173. *Cf. Lough*, 221 F. Supp. 3d at 773 (explaining that information secured by the NIT was transferred to FBI via internet).

174. *See* United States v. Jones, 565 U.S. 400, 405 (2012) (acknowledging a close connection between property law and Fourth Amendment jurisprudence). Justice Scalia wrote,

> The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous. Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass . . . .

Id. (citations omitted)

175. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000) (holding that electronic signals are enough to establish trespass action); America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (holding that even without physical damage to computer, unwanted spam still trespass); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (holding these is a viable claim for trespass when the defendant sends unwanted electronic signals to the plaintiff's network); Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1566 (1996) (holding that it is a trespass to "hack" into computer system to make free long distance telephone calls); Washington v. Riley, 846 P.2d 1365 (Wash. 1993) ("[A] person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another[.]" (quoting WASH. REV. CODE § 9A.52.110 (repealed 2016))).

176. *See eBay, Inc.*, 100 F. Supp. 2d at 1071 (holding that even a very small percentage of unauthorized usage constitutes trespass because it is still use of another person's property). *But see* Intel Corp. v. Hamidi, 71 P.3d 296, 309, 312 (Cal. 2003) (holding that some level of actual damage to a computer system is necessary to establish cause of action for trespass).

177. *Cf.* United States v. Jean, 207 F. Supp. 3d 920, 928 (W.D. Ark. 2016) (noting that the NIT downloaded and did its job so quickly that it would have been unnoticeable by the owner of computer); *see also* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 79-82 (2003) (explaining the idea of trespass in the digital realm).

178. *See* New York v. Class, 475 U.S. 106, 111 (1986) (stating that even very small physical intrusions can constitute a search under the Fourth Amendment); *Lough*, 221 F. Supp. 3d at 773 (describing how the FBI deployed NIT on Lough's computer without his

VI. LOGGING OFF: IMPACT AND MORE QUESTIONS TO CONSIDER

The digital age has revolutionized the way the world does business, learns, communicates, and thinks; this technological boom has been less effective in forcing a legal evolution.[179] Indeed, as Justice Sotomayor stressed in her concurring opinion in *Jones*, it is critical that courts be willing to adapt their understanding of the Fourth Amendment to new technologies or they risk becoming antiquated.[180] Specifically, the analysis under *Katz* likely requires reconsideration of what society truly expects in terms of online privacy.[181] This area of law is a new frontier, and the decisions made by courts like *Lough* will determine the way lawyers and government agents interact with the Constitution, thus changing the way the world operates.[182]

It is important to note that, although *Lough* failed to consider the *Jones* Fourth Amendment test, it does not necessarily mean the NIT violated the Constitution.[183] Indeed, *Lough* and the majority of its companions found that the warrant used to authorize the NIT was sufficient.[184] Thus, although the NIT was a search, it was a warranted one.[185]

Yet, the prospect of these types of "mass warrants" is still frightening to those concerned with protecting individual liberties.[186] One fear is that law enforcement tools like the NIT are a slippery slope; if the FBI can forcibly place code on a person's computer, what else can it do?[187] The FBI has attempted to

---

knowledge); *eBay, Inc.*, 100 F. Supp. 2d at 1071 (setting the amount of resource use necessary for cybertrespass is very low).

179. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (holding just three years ago that cellphones were categorically different than other types of information containers, such as cigarette packets); *see also Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) (expressing that the Supreme Court may need to update its thinking with regard to Fourth Amendment search analysis in order to keep pace with the evolution of technology and its interaction with society).

180. *See Jones*, 565 U.S. at 418 (expressing "doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every web site they had visited").

181. *See id.* at 418 ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited for the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." (citations omitted)).

182. *See supra* notes 13–15 and accompanying text (explaining that the United States Supreme Court's Fourth Amendment jurisprudence in the physical world is well defined, but digital world jurisprudence in nearly non-existent).

183. *See Lough*, 221 F. Supp. at 778 (finding that the warrant authorizing NIT was sufficient); *see also* U.S. CONST. amend. IV (providing protections against warrantless searches and seizures).

184. *See* United States v. Jean, 207 F. Supp. 3d 920, 938 (W.D. Ark. 2016) (tallying numerous *Lough* companion cases finding the warrant to have been adequate to authorize NIT).

185. *See Lough*, 221 F. Supp. 3d at 778 (comparing the NIT to a GPS tracker and concluding that the NIT warrant complied with federal law).

186. *See* Nakashima, *supra* note 1 ("As the hacking techniques become more ambitious, failure in execution can lead to large-scale privacy and civil liberties abuses at home and abroad.").

187. *See id.* (expressing concern about NIT's future impact).

quell these concerns by stating the NIT is only to be used against those taking actions to download child pornography; therefore, it would be highly unlikely for a truly innocent person to come into contact with the NIT.[188] Nevertheless, in a post-Snowden world, it is all too common for the public to harbor distrust of covert government actions.[189]

188. *See id.* ("[T]he bureau recognizes that the use of an NIT is 'intrusive' and should only be deployed 'in the most serious cases.' [The quoted FBI agent] said the FBI uses the tool only against offenders who are 'the worst of the worst.'").

189. *See* NPR Staff, *supra* note 42 (explaining that Tor usage increased after Snowden's revelation of NSA techniques).