St. Mary's Law Journal

Volume 49 | Number 1 Article 3

1-1-2017

Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine

Eduardo R. Mendoza
St. Mary's University School of Law

COMMENT

NETWORK INVESTIGATION TECHNIQUES: GOVERNMENT HACKING AND THE NEED FOR ADJUSTMENT IN THE THIRD-PARTY DOCTRINE

EDUARDO R. MENDOZA*

* This Comment is dedicated to the author's loving grandparents, Alicia "Licha" Mendoza (1935–2017) and Esteban Mendoza (1933–2017). The two met in the sixth grade and were married for 64 years before passing just eight months apart from each other. May they Rest in Peace.

I. INTRODUCTION

Our world has evolved. Modern society is largely dependent on technology, wireless devices, and the never-ending appetite for scientific development. Legal discovery is no longer limited to hard-copy, tangible documents.[1] Property interests are no longer exclusive to personal and real property.[2] The First Amendment no longer limits its protection to solely written or spoken words.[3] Our world has evolved, and the law has adjusted accordingly.

What remains constant is the yearning for truth. The clash of technology and the law is an exciting, yet dangerous phenomena. It is dangerous because society needs a justice system that seeks truth, yet desperately needs technological progress. What results when our thirst for truth conflicts with the scientific changes for which we so frantically ask? The answer has typically been adjustment.[4]

---

1. *See, e.g.*, Brandon M. Kimura & Eric K. Yamamoto, *Electronic Discovery: A Call for a New Rules Regime for the Hawai'i Courts*, 32 U. HAW. L. REV. 153, 155 (2009) (presenting the arrival of electronic discovery as a "technology revolution" transforming modern discovery).

2. *Cf.* Bd. of Trs. v. Roche Molecular Sys., Inc., 563 U.S. 776, 785 (2011) (recognizing the notion that "[a]lthough much [of] intellectual property law has changed in the 220 years since the first Patent Act," the premise that "inventors have [a] right to patent their inventions has not").

3. *See, e.g.*, Texas v. Johnson, 491 U.S. 397, 397 (1989) (finding the burning of the American flag to be "expressive conduct within protection of [the] First Amendment").

4. *See* Kyllo v. United States, 533 U.S. 27, 35 (2001) (rejecting a "mechanical interpretation of the Fourth Amendment" in the face of "advancing technology"); United States v. Davis, 785 F.3d 498, 537 (11th Cir. 2015) (Martin, J., dissenting) (recognizing a "slippery slope . . . would result from a wooden application of the third-party doctrine[,]" and further identifying such as an explanation for the insistence of the Supreme Court "that technological change sometimes requires us to consider the scope of decades-old Fourth Amendment rules" (citing *Kyllo*, 533 U.S. at 35)); *cf.* Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."). Another example is the case *Riley v. California*, 134 S. Ct. 2473 (2014). There, the Court was asked to decide whether the decades-old "search-incident-to-arrest" exception to the warrant requirement applied to cell phones on an arrestee's person. Riley v. California, 134 S. Ct. 2473, 2481 (2014) ("[T]he Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person." (citing California v. Diaz, 244 P.3d 501, 505–06 (2011)); *see also*

The Fourth Amendment's protection is largely governed by the reasonable expectation of privacy.[5] Therefore, the Fourth Amendment *demands* adjustment; a reasonable expectation of privacy, without adjustment to modern trends, is not reasonable at all.[6] Indeed, "we must never forget that it is a *constitution* we are expounding."[7] As the late Justice Scalia noted, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment [would be] entirely unaffected by the advance of technology."[8]

Accordingly, this Comment aims to signal a need for an adjustment in the Fourth Amendment's third-party doctrine, while also analyzing government hacking in relation to the Fourth Amendment. Section I will provide an overview of government hacking. Section II will provide a brief history of the Fourth Amendment. Section III will discuss software used to conceal an IP address and Fourth Amendment implications. Section IV will analyze the Western District of Texas's approach to IP address concealing software. Section V will examine the third-party doctrine. Section VI will demonstrate the need for Supreme Court guidance on the third-party doctrine in a digital age. Section VI will also propose a small framework for courts to follow until the Supreme Court re-visits the third-party doctrine. The Comment concludes with final thoughts in Section VII.

This Comment will not examine Rule 41(b)[9] and its forthcoming amendment.[10] The proposed amendment is limited in scope and will not

---

id. at 2495–96 (Alito, J., concurring in part and concurring in the judgement) (discussing the origins of the search-incident-to-arrest rule and how it relates to cell phones and personal privacy with modern technology). California argued the Court's decade-old law controlled the decision. *See id.* at 2485 (majority opinion) (suggesting, without deciding, "that a search of cell phone data might help ensure officer safety" but the parties failed to "suggest that their concerns [were] based on actual experience"). But the *Riley* Court reasoned that cell "phones are based on technology nearly inconceivable just a few decades ago, when [the law was] decided." *Id.* at 2484. Accordingly, Fourth Amendment analysis has typically adjusted as technology advances over time.

5. *See Katz*, 389 U.S. at 360 (Harlan, J., concurring) ("[A] person has a constitutionally protected reasonable expectation of privacy[.]").

6. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (arguing the Fourth Amendment requires consistent monitoring of technology's effects on privacy).

7. *See* M'Culloch v. Maryland, 17 U.S. 316, 407 (1819) (explaining how the text of the Constitution does not include every possible interpretation as, for example, a statute would).

8. *Kyllo*, 533 U.S. at 33–34.

9. FED. R. CRIM. P. 41(b) (discussing search and seizure procedure).

10. *See* ADVISORY COMM. ON CRIMINAL RULES, REPORT OF THE ADVISORY COMMITTEE ON CRIMINAL RULES 67–71 (2016) (proposing an amendment to Rule 41(b)).

address constitutional questions.[11] Constitutional standards will be left to "ongoing case law development."[12] Instead, this Comment will analyze the Fourth Amendment as it applies to government hacking, a user's expectation of privacy while browsing with concealing software, the varying rationales of the courts, and the need for adjustment in the third-party doctrine.

II. GOVERNMENT HACKING—NETWORK INVESTIGATION TECHNIQUES

The clash between scientific advancement and the search for truth has recently taken an interesting form—government hacking. The United States Government has increasingly used Network Investigation Techniques (NITs) to target suspects in criminal investigations.[13] A NIT is a hacking method used to identify criminal suspects shielding their identity with anonymous servers.[14] To put things into perspective, imagine a criminal suspect browsing the Internet. The suspect utilizes software, which conceals his or her Internet Protocol Address (IP address), and browses the Internet anonymously. Later, the FBI uses a NIT to decipher the suspect's concealed IP address. The FBI intends to use the decoded IP throughout their investigation. Must they have obtained a warrant before obtaining the IP address?

Essentially, this is how NITs operate—they identify criminal suspects who have taken affirmative steps to conceal their identity while browsing

11. *See id.* at 69 (explaining the revision of Rule 41(b) makes clear that the rule "identifies courts that may consider an application for a warrant, not the constitutional requirements for the issuance of a warrant, which must still be met").

12. *Id.* at 71.

13. *See* United States v. Werdene, 188 F. Supp. 3d 431, 440 (E.D. Pa. 2016) ("A number of federal courts have recently issued opinions in cases arising from [a] NIT application[.]"); *see also* United States v. Matish, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016) ("Defendant seeks to suppress 'all evidence seized from Mr. Matish's home computer by the FBI . . . through the use of a network investigative technique . . . ."); United States v. Levin, 186 F. Supp. 3d 26, 26 (D. Mass. 2016) (addressing the use of the NIT in a child pornography case, which traced an IP address to the suspect's home); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) (denying a motion to suppress evidence gathered by a NIT); United States v. Stamper, No. 1:15cr109, 2016 WL 695660, at *2 (S.D. Ohio Feb. 19, 2016) (explaining the scope of the Fourth Amendment as it relates to government hacking); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *3 (W.D. Wash Jan. 28, 2016) (addressing how the FBI utilized a NIT to collect an "IP address, MAC address, and other computer-identifying information").

14. *See* Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED (April 16, 2009, 9:33 PM), http://www.wired.com/2009/04/fbi-spyware-pro/ [https://perma.cc/8Z2S-7857] ("The software's primary utility appears to be in tracking down suspects that use proxy servers or anonymizing websites to cover their tracks.").

the Internet. The hacking technique has become especially useful to government officials attempting to capture criminal suspects utilizing the "dark web."[15] Unclear, however, is whether a NIT falls within the scope of a Fourth Amendment search when deployed against a user intentionally shielding his or her IP address.[16]

III. A BRIEF OVERVIEW OF THE FOURTH AMENDMENT

A. *The Property Approach*

The Fourth Amendment commands "the people be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[17] On its face, the Fourth Amendment protects two types of expectations: one involving searches, the other involving seizures.[18] This Comment focuses on searches.

The Fourth Amendment has endured intense scrutiny, which has often

15. *See* David Glance, *Explainer: What is the Dark Web?*, THE CONVERSATION (Aug. 13, 2015, 1:28 AM), http://theconversation.com/explainer-what-is-the-dark-web-46070 [https://perma.cc/4VM8-M9SK] ("The 'dark web' is a part of the world wide web that requires special software to access. Once inside, websites and other services can be accessed through a browser in much the same way as the normal web."). Because the dark web affords anonymity, it is a common "choice for groups wanting to stay hidden online from governments and law enforcement agencies . . . [and is frequently] used by paedophile groups, terrorists and criminals to keep their dealings secret." *Id.*

16. *See* Adam Shepherd, *FBI Needs a Warrant to Hack Your Computer, Judge Rules*, IT PRO (Sep 12, 2016), http://www.itpro.co.uk/security/27222/fbi-needs-a-warrant-to-hack-your-computer-judge-rules [https://perma.cc/V5VS-E776] ("Legal opinion on this topic has been divided, however, and as part of a case relating to the same FBI operation, a Virginia District Judge ruled that the government needed no warrant in order to hack a defendant's computer."). If no warrant is needed, it follows that government hacking is not a search. *See* United States v. Darby, 190 F. Supp. 3d 520, 527–28 (E.D. Va. 2016) ("If the use of the NIT was not a search, the Fourth Amendment was not implicated, [and] no warrant was required[.]"). On the other hand, if a NIT is a search, the Fourth Amendment would require a warrant. U.S. CONST. amend. IV; *see also* Laura Wagner, *Federal Judge Rules FBI Can't Hack Someone's Computer Without Warrant*, SLATE (Sept. 12, 2016, 5:13 PM), http://www.slate.com/blogs/future_tense/2016/09/12/federal_judge_rules_fbi_can_t_hack_someone_s_computer_without_warrant.html [https://perma.cc/2F9J-PZNR] (recognizing the argument that government hacking "doesn't constitute a 'search,' and therefore doesn't require a warrant at all"); Janus Kopfstein, *Federal Judge: Hacking Someone's Computer is Definitely a 'Search'*, MOTHERBOARD (Sept. 11, 2016, 10:00 AM), http://motherboard.vice.com/read/hacking-is-a-search-according-to-federal-judge (pointing to court splits on the issue); Ali Breland, *Judge Rules a Police Hack Can be a Search*, THE HILL (Sept. 12, 2016, 10:52 AM), http://thehill.com/policy/technology/295406-judge-rules-a-police-hack-can-be-a-search [https://perma.cc/Z4PG-TUY9] (recognizing a judge's ruling that government hacking was "unquestionably a 'search' for Fourth Amendment purposes").

17. U.S. CONST. amend. IV.

18. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

resulted in adjustment, restriction, or expansion of its purview.[19] Early "Fourth Amendment jurisprudence was tied to common law trespass . . . until the latter half of the 20th century."[20] A shining example is the case *Olmstead v. United States*,[21] where then Chief Justice Taft reasoned a wiretap was not a search because it did not violate Olmstead's property rights.[22] Under *Olmstead*, a NIT would not be considered a search because NIT applications are free of intrusion on a person's physical property.[23]

Ironically, *Olmstead* also stands for the demise of the property approach. As one commentator notes, the Supreme Court rejected the "property-based view" in part because of Justice Brandeis's dissent.[24] Brandeis explained that although the Constitution is enacted from an "experience of evils," a Fourth Amendment interpretation should not be restricted to the form such evils have taken, because as time passes, evil takes new forms.[25] The dissent expressed a need for a flexible interpretation of the amendment; a provision affording individual protection against a specific abuse of power could not be limited to the society surrounding the hands that drafted it.[26] If the Fourth Amendment is to offer any protection at all, it must be capable of adjustment.[27] Rightfully, *Olmstead* is no longer the law.[28]

---

19. *See, e.g.*, United States v. Jones, 565 U.S. 400, 405 (2012) (explaining the evolution of Fourth Amendment jurisprudence regarding trespass law); *see also* Ontario v. Quon, 560 U.S. 746, 759 (2010) (describing how "[t]he Court must proceed with care when considering . . . privacy expectations in communications" because of a possible risk of error due to "emerging technology" in society).

20. *Jones*, 565 U.S. at 405 (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)).

21. Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

22. *See id.* at 466 (reasoning wiretapping was not a "search or seizure within the meaning of the Fourth Amendment" as there was no physical entry).

23. *See id.* (holding precedent, at that time, required there be "an official search and seizure" of a person's tangible material, "or an actual physical invasion of his house").

24. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 817 (2004) (recognizing existing scholarship supporting the notion that the Supreme Court rejected *Olmstead*'s property-based approach in echo of Justice Brandeis's dissent).

25. *See Olmstead*, 277 U.S. at 472–73 (Brandeis, J., dissenting) ("Time . . . brings into existence new conditions and purposes.").

26. *See id.* at 472 ("Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.").

27. *See id.* at 473 ("[A] principal to be vital must be capable of wider application than the mischief which gave it birth.").

28. *See* Alderman v. United States, 394 U.S. 165, 191 (1969) (Harlan, J., concurring in part and dissenting in part) (declaring *Olmstead* "is no longer the law"); *see also* Desist v. United States, 394 U.S. 244, 278 (1969) (Fortas, J., dissenting) ("Thus, although a closely divided Court supposed in [*Olmstead*] that surveillance without any trespass and without the seizure of any material object fell outside the

B. *The Reasonable Expectation of Privacy*

Rejecting *Olmstead*'s approach, *Katz v. United States*[29] revolutionized Fourth Amendment jurisprudence when Justice Harlan declared the Fourth Amendment protects reasonable expectations of privacy.[30] In *Katz*, Justice Harlan set forth a two-pronged test for determining whether a person holds the requisite expectation under the Fourth Amendment: first, a person must exhibit "an actual (subjective) expectation of privacy[;]"[31] and second, the expectation must "be one that society is prepared to recognize as 'reasonable.'"[32] Despite a ground-breaking framework, society continues to advance, catapulting complex issues into courts across the country. Applying the law to rapid advancements in technology is not as straight-forward as it may have once been.

IV. THE ONION ROUTER AND THE ANONYMOUS IP ADDRESS

As previously mentioned, a NIT is especially helpful in attempting to capture criminal suspects utilizing the dark web.[33] Accessing the dark web requires software which conceals a user's IP address.[34] It is helpful to understand how an IP address works before discussing Fourth Amendment implications.

A. *The IP Address*

An internet protocol address (IP address) "is a unique identifying number given to every single computer on the Internet."[35] This identifying number

ambit of the Constitution, we have since departed from the narrow view on which that decision rested."); *see also* Jones v. United States, 362 U.S. 257, 266 (1960) (articulating why "it is unnecessary and ill-advised" to have *Olmstead* as the law, when the law has been "developed and refined by the common law"), *overruled by* United States v. Salvucci, 448 U.S. 83 (1980). *But see* Mitchell v. Forsyth, 472 U.S. 511, 531 (1985) (citation omitted) ("[A]lthough the rule in *Olmstead* had suffered some erosion, the Court had never explicitly disavowed it." (citing Silverman v. United States, 365 U.S. 505 (1961))).

29. Katz v. United States, 389 U.S. 347 (1967).

30. *Id.* at 360 (Harlan, J., concurring).

31. *Id.* at 361.

32. *Id. But see* United States v. Jones, 565 U.S. 400, 409 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

33. *See* Glance, *supra* note 15 (discussing the concept of the "dark web," where certain websites are hidden, and thus become a common choice for pedophile, terrorist, and criminal groups seeking to evade law enforcement agencies).

34. *See* United States v. Werdene, 188 F. Supp. 3d 431, 437 (E.D. Pa. 2016) (expounding on the deployment of a NIT used to combat a suspect accessing the dark web); *see also* Glance, *supra* note 15 (explaining the need for special software to access the dark web).

35. Paul Gil, *IP Addresses, Explained: How IP Addresses Work on the Web*, LIFEWIRE,

is akin to a license plate on a car—"it shows ownership, allows the machine to be located by other machines, and empowers authorities to track and protect people's safety, if need be."[36] Typically, when a user attempts to visit a webpage, a request is sent out to that webpage, and the information sought is sent back to the user's IP address.[37]

In effect, the Internet is a hierarchy of networks simultaneously distributing identification information.[38] When a user types a URL into a web browser, the browser contacts a specific server in order to obtain the user's IP address.[39] That specific server then sends a "query" to the URL's server, inquiring into whether the URL server knows the IP address for the website the user is trying to visit.[40] If the server for the URL knows the IP address for the target website, it returns the website's IP address to the URL server.[41] Finally, the URL server returns the website's IP address to the user's browser and the webpage appears.[42] This process is repeated each time a user visits a webpage.[43]

Therefore, a user wishing to cloak their online identity must bypass the complicated web of global networks and abstract procedures described above.[44] One way of achieving this is through software like "TOR"—an acronym for "The Onion Router."[45]

---

https://www.lifewire.com/how-ip-addresses-work-on-the-web-2483446 [https://perma.cc/Z4PG-TUY9)].

36. *Id.*

37. *See IP 101: The Basics of IP Addresses*, WHATISMYIPADDRESS.COM, [hereinafter *IP 101*], http://whatismyipaddress.com/ip-basics [https://perma.cc/N96M-RTVF] (declaring an IP address holds "a significant role" between a computer and the internet).

38. *See* Jeff Tyson, *How Internet Infrastructure Works*, HOWSTUFFWORKS (Apr. 3, 2001), http://computer.howstuffworks.com/internet/basics/internet-infrastructure1.htm [https://perma.cc/4KCY-5GUY] (characterizing the internet as "simply a network of networks").

39. *See id.* (describing the interaction between a browser and an IP address).

40. *See id.* (providing an example of a query in conjunction with a visit to a website).

41. *See id.* (detailing the process once an IP address has been identified by a server).

42. *See id.* (concluding the process governing the interplay of browser, server, and IP address).

43. *See IP 101*, *supra* note 37 ("When you go online for email, to shop or chat, your request has to be sent out to the right destination, and the responses and information you want need to come back directly to you. An IP address plays a significant role in that.").

44. *See* Tyson, *supra* note 38 (describing the Internet as a "global collection of networks, both big and small").

45. *See* Glance, *supra* note 15 ("There are a number of ways to access the dark web, including the use of Tor . . . one of the easiest software packages to use."); *see also* United States v. Broy, 209 F. Supp. 3d 1045, 1049 (C.D. Ill. 2016) (explaining how TOR works to "mask a user's IP address").

B. *The Onion Router*

TOR allows users to "view, upload and share [information] without being identified by traditional law enforcement investigative methods."[46] When someone uses software like TOR, the software masks the user's IP address with the help of volunteers around the world:

> When first logging into the Tor network, a user, whether knowingly or not, communicates his or her IP address to the first node volunteer. It is only after an IP address has been routed through multiple nodes that a user's IP address becomes masked. Indeed, when a user finally accesses a website while logged into the Tor network, only the IP address of the "exit node" is visible to that site (and to any law enforcement officials monitoring that site). Traditional investigative techniques are therefore ineffective in finding a Tor user's real IP address.[47]

Stated simply, TOR routes IP addresses through a network of volunteer computers called "nodes" to mask the original user's IP address. As a result, it is nearly "impossible to trace the IP address back to the originating computer."[48] Consequently, a user browsing with TOR holds at least a subjective expectation of privacy,[49] for the entire purpose behind TOR is to remain anonymous.[50] A subjective expectation of privacy satisfies the first prong in Justice Harlan's two-pronged test.[51] What this Comment discusses is applicable to the second prong: is society ready to accept this expectation of privacy as objectively reasonable?[52]

---

46. United States v. Werdene, 188 F. Supp. 3d 431, 435 (E.D. Pa. 2016).

47. *Broy*, 209 F. Supp. 3d at 1049; *see also* Glance, *supra* note 15 ("Tor provides secrecy and anonymity by passing messages through a network of connected Tor relays, which are specially configured computers."). The article explains how TOR sends a message, which "hops from one node to another" while encryption ensures only the receiving node "knows about the machine that sent the message." *Id.*

48. *Werdene*, 188 F. Supp. 3d at 437. *But see* Glance, *supra* note 15 ("It is a mistake to think that Tor is entirely anonymous. If a web site is accessed, it can still potentially find out information about whoever is accessing the site because of information that is shared, such as usernames and email addresses. Those wanting to stay completely anonymous have to use special anonymity services to hide their identity in these cases.").

49. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) (reasoning a TOR user "hopes for, if not possesses, a subjective expectation of privacy in his or her identifying information").

50. *See id.* (taking note of TOR marketing itself as a location hiding tool).

51. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (delineating the actual, subjective expectation of privacy requirement).

52. *See id.* (illustrating the principle with the example of public conversations where one

V. THE WESTERN DISTRICT OF TEXAS

Addressing a novel issue without circuit court precedent,[53] district courts across the country are producing split opinions.[54] The issue reached the Western District of Texas in 2016.

A. *The IP Address Is of No Import?*

In *United States v. Torres*,[55] the court held that locating a criminal suspect's IP address through the use of a NIT constituted a search implicating the Fourth Amendment.[56] A website ("Website A") operated as a hidden service under TOR to advertise and distribute child pornography.[57] Specifically, Website A "hosted 95,148 posts, 9,333 topics, and 158,094 members[.]"[58] To combat this, the FBI began to operate Website A from a government server as part of an investigation.[59] Eventually, the FBI deployed a NIT, which caused Website A's users to disclose certain information when they logged on to the website.[60] The information included the user's "IP address . . . a unique identifier generated by the NIT

possesses no objectively reasonable expectation of not being overheard).

53. Only district courts have addressed the TOR network and its Fourth Amendment implications.

54. *See* Kopfstein, *supra* at note 16 ("Courts across the country can't seem to agree on whether the FBI's recent hacking activities ran afoul of the law . . . . Some [courts] argu[e] that hacking doesn't constitute a 'search,' and therefore doesn't require a warrant at all."); *see also* C. Aliens, *Judge: FBI Playpen Hack Is "Unquestionably" a Search Under Fourth Ammendment*, DEEPDOTWEB (Sept. 25, 2016), https://www.deepdotweb.com/2016/09/25/judge-fbi-playpen-hack-unquestionably-search-fourth-ammendment/ [https://perma.cc/6QNY-7ZTB] ("[U]ntil now, no judge has ruled that law enforcement hacking is considered a search under the Fourth Amendment. Previous judges made their decision based on the defendant's lack of 'reasonable expectation of privacy.'"); Joseph Remines, *"Hacking Someone's Computer is Definitely a Search"*, THE MERKLE (Sept. 11, 2016), http://themerkle.com/hacking-someones-computer-is-definitely-a-search/ [https://perma.cc/G8UJ-MCKE] (writing about how "[a] federal judge in Texas ruled that sending malware to someone's computer without their prior knowledge is classified as a search under the [Fourth] Amendment" but that a Virginia judge ruled "a warrant wasn't even needed for government hacking purposes"); *see also* Greg Masters, *FBI Sweep: It's a Search, Get a Warrant, Says Fed Judge*, SC MAGAZINE (Sept. 14, 2016), https://www.scmagazine.com/fbi-sweep-its-a-search-get-a-warrant-says-fed-judge/article/529536/ [https://perma.cc/SV94-S2BT] ("The legality of FBI investigations using a NIT warrant has previously been questioned with courts in different jurisdictions issuing conflicting rulings.").

55. United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016).

56. *See id.* at *3 ("This was unquestionably a 'search' for Fourth Amendment purposes.").

57. *Id.* at *1 (W.D. Tex. Sept. 9, 2016).

58. *Id.*

59. *Id.* at *2.

60. *Id.*

to distinguish . . . users from one another, and the operating system of the [user's] computer."[61] As a result, when Torres logged onto Website A, the NIT was triggered and released Torres's IP address to investigators.[62] At that point, the FBI linked the disclosed IP address to a certain Internet service provider and subpoenaed that provider.[63] In turn, the subpoenaed information led investigators to Torres, and he was arrested.[64] Despite the intricate use of the IP address and the extensive process used to identify its owner, the court reasoned an IP address did not afford a reasonable expectation of privacy, and was, therefore, irrelevant to the analysis.[65]

Instead, the court swiftly focused its attention on the expectation of privacy in Torres's *computer*.[66] Concluding it was of "no import" that Torres may have a reasonable expectation of privacy in his IP address,[67] the court proceeded to compare Torres's computer to a cellphone.[68] The argument was that just as a user holds a reasonable expectation of privacy in their cellphone, a user also holds the same expectation in their computer.[69] The holding required the government to obtain a warrant before issuing the NIT.[70]

Although the court's reasoning is thorough, its analysis is open to criticism. For example, it is true the Fourth Amendment *may* protect content stored on a cellphone—the protection stems from the word

61. *Id.*

62. *Id.*

63. *See id.* (issuing a subpoena for records from Time Warner Cable, which lead to the discovery of Mr. Torres's IP address).

64. *Id.*

65. *Id.* at *3.

66. *See id.* (emphasizing Torres's "expectation of privacy in his IP address [was] of no import").

67. The court noted that one holds no reasonable expectation of privacy in their IP address, even while using TOR. *See id.* ("[C]ourts—both those to address the issue in the context of the NIT warrant and those addressing the issue in the context of IP addresses more generally, have consistently found that there is no reasonable expectation of privacy in an IP address itself, even when using a Tor browser." (citing United States v. Darby, 190 F. Supp. 3d 520, 528–29 (E.D. Va. 2016))). This led to the court's determination that Torres's IP address was of "no import" to the analysis. *Id.*

68. *See id.* (applying the Supreme Court's reasoning that "due to the extensive amount of personal information contained" within both a cell phone and a computer, a similar expectation of privacy should apply).

69. *See id.* (positing the idea that because the Supreme Court has held "individuals have a reasonable expectation of privacy in their cell phones," the same logic applies to computers (citing Riley v. California, 134 S. Ct. 2473, 2485 (2014))).

70. *See id.* (adopting the conclusion that despite any lack of expectation of privacy, the use of the NIT by the government was a search according to the Fourth Amendment).

"papers" within the amendment itself.[71] The word "papers" affords protection for "private information . . . store[d] on digital devices[,]" which may encompass a cellphone.[72] Typically, there is a vast amount of personal information on cellphones, and the Supreme Court has afforded such content a reasonable expectation of privacy.[73]

Nonetheless, the *Torres* court's analysis is devoid of case law *withholding* Fourth Amendment protection from non-content information.[74] The Supreme Court has distinguished content from non-content information.[75]

---

71. *See Riley*, 134 S. Ct. at 2494–95 (explaining "cell phones are not just another technological convenience" because they contain "the privacies of life" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))). The Court explains that just because "technology now allows an individual to carry such information in his hand does not [mean] the information [is] any less worthy of the protection for which the Founders fought." *Id.* at 2495. The Court further made clear that police officers must obtain a warrant before searching cell phones incident to arrest. *See id.* ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."); *see also* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (stressing the importance of either a warrant or particularized suspicion to examine, in depth, the contents of a computer at the border). In *Cotterman*, the Ninth Circuit credited our Founders for incorporating "papers" within the Fourth Amendment, which was interpreted to include "papers we create and maintain not only in physical but also in digital form[.]" *Id.* at 957.

72. *See Cotterman*, 709 F.3d at 964 (indicating electronic devices satisfy Justice Harlan's two-prong test, because such devices simultaneously serve as "offices and personal diaries"); *see also* United States v. Turner, 839 F.3d 429, 435–36 (5th Cir. 2016) (analyzing the reasonable expectation of privacy in a gift card by comparing them to cell phones, noting "[a] primary purpose of modern cell phones, and certainly of computers, is to store personal information").

73. *See, e.g.*, *Riley*, 134 S. Ct. at 2485 (reasoning that because cell phones "place vast quantities of personal information literally in the hands of individuals[,]" the Fourth Amendment demands a warrant before an officer conducts a search).

74. *Accord* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (recognizing the Fourth Amendment does not protect "phone numbers" disclosed to phone companies and "e-mail addresses" disclosed to service providers, because the information is non-content); *see Ex parte Jackson*, 96 U.S. 727, 733 (1877) (distinguishing between a search of the "outward form" of mail, which does not require warrant, versus a search of the contents within, which does); *see also* United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016) ("What Defendants fail to recognize is that for each medium of communication these cases address, there is also a case expressly withholding Fourth Amendment protection from non-content information, i.e., information involving addresses and routing." (citing *Jackson*, 96 U.S. at 733)); *see also* United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) (referring to the modern-day letter—the email—as holding similar protections under the Fourth Amendment, while simultaneously accepting the lack of any reasonable expectation of privacy in non-content information, such as an IP address (citing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010))).

75. *Compare* Katz v. United States, 389 U.S. 347, 353 (1967) (emphasis added) (holding that "[t]he Government's activities in electronically listening to and recording the petitioner's *words*" was a search under the Fourth Amendment), *with* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding the police's installation of a pen register—a device that tracked the phone numbers a person dials—was not a search.). The Court, in *Smith*, explained: "Although [the caller's] conduct may have been

Content information enjoys Fourth Amendment protection, while non-content information does not.[76] Therefore, although a cellphone and a computer may be similar, the similarity is nullified for Fourth Amendment purposes if the information obtained is non-content.[77] In light of this distinction, a critic might argue the court should have inquired into whether the information obtained through the NIT was "content information" before concluding that all information on a user's computer is "content" just because of the similarities between computers and cellphones.

B. *Content v. Non-Content*

Let us revisit the facts in *Torres*: the information obtained through the NIT was Torres's IP address, a unique identifier and the operating system for Torres's computer.[78] To be clear, the NIT did not gather images or other media.[79] Instead, it only gathered identifying information, such as Torres's IP address.[80] The court nonetheless reasoned a violation occurred because Torres had a reasonable expectation of privacy in the "content" of his computer.[81] Because the NIT only gathered identifying information like

calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Smith*, 442 U.S. at 743; *see also Graham*, 824 F.3d at 433 (tracing the history of the Supreme Court's distinction between content and non-content information in communications). In *Graham*, the Fourth Circuit adopted the reasoning of the Sixth Circuit, recognizing that CSLI is non-content information because "cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves." *Id.* (quoting *Carpenter*, 819 F.3d at 887–88).

76. *See Graham*, 824 F.3d at 433 ("The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content."); *see also Riley*, 134 S. Ct. at 2485 (deciding the vast amount of information contained within a cellphone demands a warrant be required before a search is conducted); *see also Jackson*, 96 U.S. at 733 (clarifying the distinction between a search of the outward appearance and weight of an envelope versus an inward search of the contents contained therein).

77. *See Graham*, 824 F.3d at 433 (explaining how "mailing addresses, phone numbers, and IP addresses" are non-content information, and thereby precluded from Fourth Amendment protection).

78. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *2 (W.D. Tex. Sept. 9, 2016) ("[The NIT caused] the 'activating' computer to send certain information to a computer run by the Government. This information included the IP address of the 'activating' computer, a unique identifier generated by the NIT to distinguish 'activating' users from one another, and the operating system of the 'activating' computer.").

79. *See id.* (emphasizing the purpose of the NIT was not to obtain content, but rather "to assist the FBI in identifying the 'activating computers' and their users").

80. *See id.* (noting the NIT caused the computer to transmit the IP address and other identifying information, not content based data).

81. *See id.* (intimating "it is reasonable to find that persons also have a reasonable expectation of

the IP address, it follows that the court believed an IP address is "content information," because the violation itself was based on intrusion into the content of Torres's computer through the NIT, which only gathered *identifying* information.[82]

But other courts have declined to extend "content" status to an IP address or other information routinely conveyed to third parties.[83] For

privacy in their personal computers, due to the vast amount of personal information they contain" (citing United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001))).

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

83. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (reiterating the notion that information conveyed to a third party, even for limited purposes, is not protected under the Fourth Amendment (citing United States v. White, 401 U.S. 745, 752 (1971)); *see also* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (rejecting a defendant's claim of a subjective expectation of privacy in his Internet subscriber information because he "voluntarily conveyed" it to a third party); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *Guest*, 255 F.3d at 336 (6th Cir. 2001) (noting "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 133 (E.D. Va. 2011) ("Even if Petitioners had a reasonable expectation of privacy in IP address information collected by Twitter, Petitioners voluntarily relinquished any reasonable expectation of privacy under the third-party doctrine."); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other non-content data to which service providers must have access." (citing *Guest*, 255 F.3d at 336 (6th Cir. 2001))); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005) (indicating most courts, for Fourth Amendment purposes, have concluded that one does not maintain a reasonable expectation of privacy in subscriber information voluntarily conveyed to Internet providers); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) ("The courts that have already addressed this issue [] uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP."); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y 2002) (recognizing individuals "have no Fourth Amendment privacy interest in subscriber information given to an [ISP]" (citing United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000))); *Kennedy*, 81 F. Supp. 2d at 1110 (rejecting a privacy interest in subscriber information revealed to third parties (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979))); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999) (finding no legitimate expectation of privacy in non-content customer information provided to an Internet service provider). The court explained, in *In re Application*, that to access Twitter, a user must voluntarily "disclose their IP addresses to third parties[,]" which implicates "significant Fourth Amendment consequences under the third-party doctrine[.]" *In re Application*, 830 F. Supp. 2d at 133; *cf.* United States v. Hernandez, 313 F.3d 1206, 1209–10 (9th Cir. 2002) (echoing a similar expectation of privacy in packages handled by mail service providers—one expects the interior to remain private while the exterior is not protected under voluntary-conveyance theory). This idea was further explained by the Ninth Circuit in *U.S. v. Forrester*,

instance, in *United States v. Hambrick*,[84] the Fourth Circuit held that while certain circumstances warrant *some* "expectation of privacy in content information, a person does not have an interest in the account information given to [an] ISP [because such information] is non-content information."[85] Similarly, an IP address is routinely provided to Internet service providers, making it non-content information.[86] This has become the essence of what is now known as the third-party doctrine, which is discussed *infra*.[87]

Despite this, the court in *Torres* felt Torres's situation was different because the NIT allegedly placed code *onto* Torres's computer without permission.[88] Because of that, the court reasoned placing a NIT *onto* Torres's computer was the search, as compared to the information acquisition itself constituting the search.[89] This reasoning probably rendered the third-party doctrine moot. Still, one might argue this reasoning is inconsistent with the court's description of how the NIT operated. The NIT was deployed so "users who accessed the target website . . . by logging in with a username and password, would be issued certain instructions, causing the 'activating' computer to send certain information to a computer run by the Government."[90] Therefore, a user was given specific instructions and took affirmative steps which caused a computer to send identifying information to the government. A user taking affirmative steps to activate the NIT would seem to preclude the argument that the NIT was placed without permission.

Furthermore, the NIT did not *attach* itself to Torres's computer, but

---

where the court articulated that an "[e]-mail, like physical mail, has an outside address 'visible' to third-party carriers[,]" thus destroying any reasonable expectation of privacy in the e-mail address once conveyed to the third party. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

84. United States v. Hambrick, No. 99-4793, 2000 WL 1062039 (4th Cir. Aug. 3, 2000).

85. *Id.* at *4 (citing *Smith*, 442 U.S. at 741).

86. *See id.* (suggesting "[d]isclosure of [] non-content information to a third party destroys the privacy expectation").

87. The third-party doctrine is more fully explained at the latter end of this Comment, at 118. In short, the third-party doctrine, also known as voluntary-conveyance theory, holds that a reasonable expectation of privacy is diminished when the subject information is conveyed to a third party. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 442 (9th Cir. 2016) ("[T]he Fourth Amendment's 'third-party' doctrine [states] that a person's privacy interest is diminished where he or she reveals information to a third party, even in confidence.").

88. United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *3 (W.D. Tex. Sept. 9, 2016).

89. *Id.*

90. *Id.* at *2.

instead signaled his computer "to *send* certain [identifying] information."[91] A NIT does not need to attach itself onto the actual computer to cause the computer to send information. And, as several courts concur, an IP address is not a component of a computer: "When a consumer purchases a computer, takes it home, opens it up, and turns it on, that computer does not have an IP address."[92] An IP address is assigned to a computer by an Internet service provider.[93] This suggests that a user's IP address can change entirely, depending on the Internet service provider.[94]

Therefore, the NIT in *Torres* could not have gathered content information from Torres's computer "without permission" if what was gathered was not a part of the computer to begin with. And when certain information is conveyed to a third party, as when an IP address is conveyed to an Internet service provider, the third-party doctrine renders the information "non-content," precluding Fourth Amendment protection.[95] This means that an IP address is non-content information for two reasons: (1) it is conveyed to a third party;[96] and (2) it is not part of a computer.[97]

---

91. *Id.* (emphasis added) (explaining how the FBI deployed a NIT, which caused website users to transmit information to a computer controlled by the FBI); *see also* United States v. Matish, 193 F. Supp. 3d 585, 617 (E.D. Va. 2016) (describing how the "[d]efendant's IP address was revealed in transit when the NIT instructed his computer to send [out] information to the FBI").

92. *See* United States v. Acevedo-Lemus, No.: SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *5 (C.D. Cal. Aug. 8, 2016); *see also Matish*, 193 F. Supp. 3d at 617 ("As the Court understands it, Defendant's IP address was not located on his computer; indeed, it appears that computers can have various IP addresses depending on the networks to which they connect.").

93. *See, e.g.*, *Acevedo-Lemus*, slip op. at *5 (recognizing an IP address as assigned by an ISP when a computer attempts to connect to a given network).

94. *See Matish*, 193 F. Supp. 3d at 617 (refuting the contention that an IP address is unique to the individual computer; rather, "computers can have various IP addresses depending on the networks to which they connect"); *cf. Acevedo-Lemus*, slip op. at *5 ("First, it does not matter that the government procured Defendant's IP address from his computer as opposed to getting it from a third party because an IP address is not a private physical feature of a computer, but a commonly disclosed digital one assigned by a third party.").

95. *See, e.g.*, United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000) ("Disclosure of [] non-content information to a third party destroys the privacy expectation that might have existed previously.").

96. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *Hambrick*, 2000 WL 1062039, at *4 (clarifying that any expectation of privacy in non-content information is destroyed upon conveyance to a third-party ISP); *Acevedo-Lemus*, slip op. at *5 (recognizing there can be no reasonable expectation of privacy in an IP address because it "is not a private physical feature of a computer, but a commonly disclosed digital one").

97. *See Acevedo-Lemus*, slip op. at *5 (emphasizing a "computer does not have an IP address" at the time a consumer purchases, receives, and opens the computer); *see also Matish*, 193 F. Supp. 3d at 617 (promoting the trend of decisions supporting the conclusion that an IP address is not a unique

To follow the court's cellphone analogy, visiting a website would be akin to dialing a phone number.[98] This similarity is important, considering the Fourth Amendment does not protect specific numbers a user dials.[99] Numbers dialed do not enjoy protection because cellphone users voluntarily convey their phone numbers to telephone companies.[100] Consequently, under the court's cellphone analogy, any expectation of privacy would be void, because what is most similar between a cellphone and a computer, as applied to Torres's case, is their comparable and consistently disclosed non-content information.

C. *Dodging the Third-Party Doctrine*

One must wonder if the *Torres* court *purposely* dodged the TOR Fourth Amendment issue. To understand this inquiry, one should question why the court would avoid addressing the issue through the usual third-party doctrine analysis mentioned before. The expectation of privacy in a user's IP address is a frequent issue, and there was plenty of precedent with which the court could work.[101]

---

feature of a computer, but one assigned by ISPs).

98. The idea is: specific numbers dialed resemble specific URLs typed into a browser. Analogously, just as an IP address identifies a user, in that the user may be located through an IP address, a user can also be located or contacted through his personal cellphone number. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (finding a similarity between IP addresses and numbers dialed). But, as discussed, numbers dialed are precluded from Fourth Amendment protection. *See Smith*, 442 U.S. at 735 (failing the test under *Katz* because "it is doubtful that telephone users in general have any expectation of privacy [in] the numbers they dial"). Therefore, the argument is that because a specific number dialed is not protected, specific URLs are not protected. And because specific URLs are not protected, via the third-party doctrine, a person's IP is likewise not protected.

99. *See Smith*, 442 U.S. at 735 (holding phone numbers dialed fails the *Katz* test for a reasonable expectation of privacy because under voluntary-conveyance theory individuals cannot reasonably expect such numbers to remain private).

100. *See id.* ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

101. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (adhering to clear Court precedent that information loses any reasonable expectation of privacy once voluntarily conveyed to a third party (citing United States v. White, 401 U.S. 745, 752 (1971))); *see also* United States v. Christie, 624 F. 3d 558, 573 (3d Cir. 2010) (recognizing many federal courts agree that "'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties" (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008))); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (rejecting the defendant's expectation of privacy because all information was voluntarily conveyed and the defendant "'assumed the risk that [those] compan[ies] would reveal [that information] to police'" (quoting *Smith*, 442 U.S. at 744)); *Forrester*, 512 F.3d at 510 (applying a similar analysis as used in *Smith*, comparing numbers

In the court's defense, *Torres* is a unique case—Torres was utilizing TOR to conceal his IP address.[102] There is not a single circuit court opinion addressing a user's reasonable expectation of privacy in their IP address while using TOR. This lack of guidance may have prompted the court to avoid the third-party doctrine and instead attempt to resolve the matter using a broader "content" analysis. That way, the court avoids addressing an unprecedented issue and potential reversal on appeal.

Here, we must think outside the box: the court refusing to rule in light of volumes of relevant precedent[103] might suggest the TOR issue is so atypical it cannot be resolved with the current third-party doctrine. Otherwise, the court would have used it. Avoiding the third-party doctrine might have been a silent call for adjustment in the law.

VI. THE THIRD-PARTY DOCTRINE IN A DIGITAL AGE

As we have seen, the Fourth Amendment issue is typically addressed under the third-party doctrine.[104] The doctrine holds that a reasonable

---

dialed to internet information provided to ISPs (citing *Smith*, 442 U.S. at 742)); *Perrine*, 518 F.3d at 1204 (approving the majority of federal courts that have addressed the issue of voluntary conveyance in conjunction with subscriber information provided to ISPs); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (declaring computer users hold no reasonable expectation of privacy in subscriber information under the voluntary-conveyance theory).

102. *See* United States v. Torres, No. 5:16-CR-282-DAE, 2016 WL 4821223, slip op. at *1 (W.D. Tex. Sept. 9, 2016) (clarifying TOR's use in this case was to cause the website's IP log to record an IP address other than the user's actual IP address, thereby concealing the user's identity).

103. *See Miller*, 425 U.S. at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." (citing *White*, 401 U.S. at 752)); *see also White*, 401 U.S. at 751–52 (1971) (analyzing the issue of whether any expectation can be reasonable when an individual voluntarily conveys information to a third party, noting that such disclosure assumes the risk that such information might be provided to police); Hoffa v. United States, 385 U.S. 293, 302 (1966) (concluding the voluntary-conveyance theory destroys any reasonable expectation of privacy under the Fourth Amendment, even when the trust in the third-party is misplaced or obtained by deception); *Christie*, 624 F.3d at 573 (using third-party doctrine to rule that subscriber information is not protected under the Fourth Amendment); *Bynum*, 604 F.3d at 164 (rejecting an expectation of privacy argument where all information was voluntarily conveyed to a third party); *Forrester*, 512 F.3d at 510 (accepting other courts' conclusions and applying the voluntary-conveyance theory to hold no expectation of privacy exists); *Perrine*, 518 F.3d at 1204 (examining the access of subscriber information under third-party doctrine and concluding that such information is devoid of Fourth Amendment protection); *Guest*, 255 F.3d at 336 (utilizing the voluntary-conveyance theory to conclude that such information is precluded from Fourth Amendment protection).

104. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 442 (9th Cir. 2016) (applying the third-party doctrine to a defendant alleging a reasonable expectation of privacy in electronic communications).

expectation of privacy is diminished when the subject information is conveyed to a third party.[105] However, in a digital age, technological advancements raise questions about the stability of this law. For instance, TOR has received special attention under the Fourth Amendment,[106] particularly because of the series of complicated steps required to use the software.[107] Some believe TOR warrants a "twist" in the third-party doctrine.[108] Others oppose treating an expectation of privacy any different because of TOR.[109]

105. *See Smith*, 442 U.S. at 742 (denying the petitioner's argument because there can be no expectation of privacy in information voluntarily conveyed to a third party); *see also* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) ("Under the third-party doctrine, an individual can claim 'no legitimate expectation of privacy' in information that he has voluntarily turned over to a third party." (quoting *Smith*, 442 U.S. at 743–44)); United States v. Turner, 839 F.3d 429, 436 (5th Cir. 2016) (adopting the reasoning of other courts using the third-party doctrine and applying it in the context of a gift card); *Mohamud*, 843 F.3d at 442 (expressing the clear precedent that voluntary conveyance of information destroys any expectation of privacy that may have existed prior to disclosure); United States v. Ackerman, 831 F.3d 1292, 1304–05 (10th Cir. 2016) ("The [Supreme] Court has, after all, suggested that individuals lack any reasonable expectation of privacy and so forfeit any Fourth Amendment protections in materials they choose to share with third parties like banks or telephone companies."); Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 823 (2d Cir. 2015) (relying on the voluntary-conveyance theory to find no reasonable expectation of privacy in public movements because they are conveyed to the public (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983))); United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (deciding there is a decreased expectation of privacy in information owned by a third party).

106. *See* Tim Cushing, *Courts, DOJ: Using Tor Doesn't Give You a Greater Expectation of Privacy*, TECH DIRT (Feb. 29, 2016, 10:41 AM), https://www.techdirt.com/articles/20160228/15011333749/courts-doj-using-tor-doesnt-give-you-greater-expectation-privacy.shtml [https://perma.cc/N9ZX-D9PY] (expressing concern in the recent decisions of federal courts which concluded IP addresses are exempt from Fourth Amendment protection without using the third-party doctrine).

107. *See* United States v. Broy, 209 F. Supp. 3d 1045, 1049 (C.D. Ill. 2016) ("In order to use the Tor network, a user must download and run Tor software on his or her personal computer. When first logging into the Tor network, a user, whether knowingly or not, communicates his or her IP address to the first node volunteer. It is only after an IP address has been routed through multiple nodes that a user's IP address becomes masked. . . . [W]hen a user finally accesses a website while logged into the Tor network, only the IP address of the 'exit node' is visible to that site[.]").

108. *See* Cushing, *supra* note 106 ("In this month alone, we've had two federal judges and the DOJ state that there's no expectation of privacy in IP addresses. This would normally be something covered by the Third Party Doctrine—where an IP address is part of the records retained by ISPs, and, therefore, can be accessed with subpoenas rather than warrants. The twist, though, is that all of these statements were made in reference to people who made an active effort to obscure their IP addresses by using Tor.").

109. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *3 (W.D. Tex. Sept. 9, 2016) (holding government use of NIT is a search).

A. *The Onion Router: Enough to Alter the Third-Party Doctrine?*

A district court in California held that TOR's requirements, despite their complication, do not alter a Fourth Amendment analysis because a TOR user still discloses an IP address to someone, somewhere.[110] The idea is that any conveyance, without regard to whom or under what circumstances the information is conveyed, is sufficient to nullify any expectation of privacy.[111] At its core, the argument is: conveying information to a third party ruins any expectation of privacy in that information, and using TOR does not change that. As a result, the question becomes: when a person uses TOR, does the software *create* a reasonable expectation of privacy where there was none before? To analyze this, it is helpful to examine similar doctrines.

The plain-view doctrine maintains that items in plain view do not enjoy a reasonable expectation of privacy.[112] The doctrine has been consistently applied by courts at all levels.[113] In particular, the doctrine applies to *any* items inside of a vehicle.[114] The Supreme Court has recognized that an

---

110. *See* United States v. Acevedo-Lemus, No.: SACR 15-00137-CJC, 2016 WL 4208436, slip op. at *6 (C.D. Cal. Aug. 8, 2016) (rejecting the proposition that TOR alters a typical Fourth Amendment analysis). The court explains:

> It also does not matter that Defendant tried to shield his IP address from the government, since he nonetheless disclosed that information to the initial Tor "entry node." As the *Werdene* court explained, "a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party"—the operator of the initial Tor node—and the fact that a user's IP address is "subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address[.]"

Id. (quoting United states v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016)).

111. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 442 (concluding that one's expectation of privacy diminishes when conveying information to a third party).

112. *See* United States v. Hunley, No. 07–CR–168A, 2010 WL 2510901, at *9 (W.D.N.Y. Feb. 26, 2010) ("[A] police officer's looking through the windows into the vehicle from outside, even when shining a flashlight to illuminate the inside of the vehicle, does not constitute a 'search' of the vehicle within the meaning of the Fourth Amendment." (quoting Mollica v. Voker, 299 F.3d 366, 369 (2d Cir. 2000))).

113. *See* New York v. Class, 475 U.S. 106, 118 (1986) (indicating places inside an automobile, situated in plain view of persons outside the vehicle, are not "subject to a reasonable expectation of privacy"); *see also* Texas v. Brown, 460 U.S. 730, 740 (1983) (citations omitted) ("There is no legitimate expectation of privacy shielding that portion of the interior of an automobile which may be viewed from outside the vehicle by either inquisitive passersby or diligent police officers."); United States v. Ocampo, 650 F.2d 421, 427 (2d Cir. 1981) (finding an item to be "in plain view" even though a police officer used a flashlight to illuminate the inside of a lawfully stopped car).

114. *See, e.g.*, United States v. Grajeda, 497 F.3d 879, 882 (8th Cir. 2007) ("While we are assuming a Fourth Amendment violation for purposes of this analysis, it is significant that we have

officer can look through the windshield of an automobile and note items in plain view without Fourth Amendment barriers.[115] The idea seems to be that once an item is openly visible to a third party, any expectation of privacy is void. However, the question is whether a person can change something about an item in plain view to *create* an expectation of privacy that did not previously exist. Typically, for the plain-view doctrine, a person taking affirmative steps to conceal an item in plain view has failed to alter plain-view doctrine analysis. This might suggest the same reasoning applies to the third-party doctrine. The following two cases describe this scenario.

B. New York v. Class

In *New York v. Class*,[116] two police officers "observed [the] respondent . . . driving above the speed limit in a car with a cracked windshield."[117] One of the officers opened the door to the respondent's vehicle in an attempt to locate the VIN, which was covered by papers.[118] The officer reached into the interior of respondent's car and moved the papers from the dashboard, where the VIN was located.[119] The Supreme Court rejected the proposition that a Fourth Amendment analysis is altered when a user takes affirmative steps to conceal their VIN number, explaining that "efforts to restrict access to an area do not generate a reasonable expectation of privacy where none would otherwise exist."[120]

---

never held that it is illegal for an officer to cross-check a VIN in both locations on a vehicle, and the Supreme Court has held that the VIN location on either the dashboard or the doorjamb is not 'subject to a reasonable expectation of privacy.'" (quoting *Class*, 475 U.S. at 118)).

115. *See Class*, 475 U.S. at 120 (Powell, J., concurring) ("[A]n officer making a lawful stop of a vehicle has the right and duty to inspect the VIN.").

116. New York v. Class, 475 U.S. 106 (1986).

117. *Id.* at 107–08.

118. *Id.* at 106.

119. *Id.*

120. *See id.* at 114 (stressing that even where a VIN has been purposely concealed, such actions fail to create a sphere of privacy (citing Oliver v. United States, 466 U.S. 170, 182–84 (1984))). The Court reasoned:

> We think it makes no difference that the papers in respondent's car obscured the VIN from the plain view of the officer. We have recently emphasized that efforts to restrict access to an area do not generate a reasonable expectation of privacy where none would otherwise exist. Here, where the object at issue is an identification number behind the transparent windshield of an automobile driven upon the public roads, we believe that the placement of the obscuring papers was insufficient to create a privacy interest in the VIN.

Id. (citations omitted).

C. Oliver v. United States

A second example is *Oliver v. United States*.[121] There, two narcotic agents received a tip "that marihuana was being [grown] on the farm of [the] petitioner . . . ."[122] When they arrived at the farm, the gate to the petitioner's home was locked and had a "No Trespassing" sign.[123] During their initial walk-through, the agents passed a parked camper from which someone shouted "[n]o hunting is allowed, come back up here[;]" but the officers continued their investigation and found a field of marijuana.[124]

Applying Justice Harlan's two-pronged test, "the District Court suppressed evidence of the discovery of the marihuana field."[125] The district court noted the petitioner had a reasonable expectation of privacy in the field because he "had done all that could be expected of him to assert his privacy in the area of the farm that was searched."[126] Of specific importance was the petitioner's posted signs, which read "No Trespassing" at intervals throughout the property, a locked gate at the entrance, and "woods, fences, and embankments" bounding the property from all sides.[127] Nonetheless, the Supreme Court rejected the district court's approach, reasoning "[t]he test of legitimacy is not whether the individual chooses to conceal assertedly 'private' activity. . . . [but] whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[128]

D. United States v. Werdene

We now return to the third-party doctrine to examine whether a person

121. Oliver v. United States, 466 U.S. 170 (1984).
122. *Id.* at 173.
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.* at 173–74.
128. *Id.* at 182–83. The Court held:

> Initially, we reject the suggestion that steps taken to protect privacy establish that expectations of privacy in an open field are legitimate. It is true, of course, that petitioner Oliver and respondent Thornton, in order to conceal their criminal activities, planted the marihuana upon secluded land and erected fences and "No Trespassing" signs around the property. . . . Neither of these suppositions demonstrates, however, that the expectation of privacy was legitimate in the sense required by the Fourth Amendment.

Id. at 182.

can *create* a reasonable expectation of privacy. In *United States v. Werdene*,[129] a criminal suspect was browsing online with TOR and encountered a NIT.[130] The FBI-deployed NIT was similar to the NIT used in *Torres*, in that it "caused software to be activated" when a user logged into a specific website, thereby causing the "user's computer to reveal its IP address to the FBI."[131] The court refused to alter the Fourth Amendment analysis, but also took its holding one step further. Relying on *Smith v. Maryland*,[132] the court reasoned that the "type of third-party" one discloses information to "does not affect the Court's evaluation of his reasonable expectation of privacy."[133]

Playing devil's advocate, a critic might argue the court relied on a faulty premise. In *Smith*, the Supreme Court did not hold that the "type of third-party" one discloses information to is of no importance. Instead, the Court analyzed a very narrow issue—whether a company, having facilities to record information disclosed by a third party, altered the analysis by *electing* to employ one program over another.[134] The argument made by the Petitioner was based on *how* a company chose to record information, not

129. United States v. Werdene, 188 F. Supp. 3d 431 (E.D. Pa. 2016).

130. *Id.* at 435. It should be noted that the *Werdene* court did not avoid addressing the user's IP address under the third-party doctrine as the court did in *Torres*. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, slip op. at *3 (W.D. Tex. Sept. 9, 2016) (addressing the content in Torres's computer, rather than his IP address, reasoning Torres's "expectation of privacy in his IP address [was] of no import"). Here, the court addressed the issue with the third-party doctrine head on. *See Werdene*, 188 F. Supp. 3d at 444 (E.D. Pa. 2016) ("Werdene had no reasonable expectation of privacy in his IP address. Aside from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party. . . .").

131. *See Werdene*, 188 F. Supp. 3d at 435 (noting the FBI's use of the NIT was to circumvent TOR).

132. Smith v. Maryland, 442 U.S. 735 (1979).

133. *Werdene*, 188 F. Supp. 3d at 444–45. The court explained:

> In *Smith*, the petitioner argued that the numbers he dialed on his telephone remained private because they were processed through automatic switching equipment rather than a live operator. . . . Similarly, the *type of third-party* to which Werdene disclosed his IP address—whether a person or an "entry node" on the Tor network—does not affect the Court's evaluation of his reasonable expectation of privacy. He was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information.

Id. (emphasis added) (first citing *Smith*, 442 U.S. at 745; then citing United States v. Farrell, No. CR15-029RAJ, 2016 WL 705197, slip op. at *2 (W.D. Wash. Feb. 23, 2016)).

134. *See Smith*, 442 U.S. at 745 (emphasis added) ("The fortuity of whether or not the phone company in fact *elects* to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference.").

the type of third party to whom the information was disclosed.[135] "Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on *how* the telephone company chose to define local-dialing zones, and depending on *how* it chose to bill its customers for local calls."[136]

In contrast, when using TOR, the issue is not *how* the Internet service provider records information, because TOR's mission is to ensure the Internet service provider records misleading information.[137] The *Werdene* court's conclusion might be open to criticism.

VII. THE THIRD-PARTY DOCTRINE IS ILL-SUITED FOR A DIGITAL AGE

Class, *Oliver*, and *Werdene* are important for two reasons. First, they suggest a privacy interest cannot be *created* by affirmative actions or certain software. Thus, as applied to a TOR user, whether a person takes affirmative steps to browse anonymously, seemingly plays no role in modern Fourth Amendment jurisprudence. On the other hand, these three cases demonstrate how novel TOR is. *Class* dealt with an *individual* attempting to cover his VIN number; *Oliver* dealt with an *individual* growing illegal drugs on his farm. TOR requires thousands of users to join together for the sole purpose of remaining anonymous. Additionally, one should recognize that the *Werdene* court likely examined *Smith*, and tried to mold its reasoning to a modern issue, namely TOR browsing. This is because the third-party doctrine has not been directly applied to digital issues by the Court. But the issue *must be addressed.* Software (like TOR) is unique—it requires a network of users[138] working simultaneously to bypass the complex web of multi-

135. *See id.* (emphasis added) ("Regardless of the phone company's *election* [of one method over another], petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.").

136. *Id.* (emphasis added).

137. *See* Jill Scharr, *What is Tor? Answers to Frequently Asked Questions*, TOM'S GUIDE (Oct. 23, 2013, 7:00 AM), http://www.tomsguide.com/us/what-is-tor-faq,news-17754.html [https://perma.cc/72CJ-VSUQ] ("[The Onion Router] is an Internet networking protocol designed to anonymize the data relayed across it. Using Tor's software will make it difficult, if not impossible, for any snoops to see your webmail, search history, social media posts or other online activity."); *see also* Glance, *supra* note 15 ("Tor provides secrecy and anonymity by passing messages through a network of connected Tor relays, which are specially configured computers. As the message hops from one node to another, it is encrypted in a way that each relay only knows about the machine that sent the message. . . .").

138. *See* Scharr, *supra* note 137 ("The Tor network runs through the computer servers of thousands of volunteers (over 4,500 at time of publishing) spread throughout the world. Your data is bundled into an encrypted packet when it enters the Tor network."); *see also* United States v. Broy, 209 F. Supp. 3d 1045, 1048–49 (C.D. Ill. 2016) ("[T]he 'Tor' network [is] an open-source software tool

dimensional networks known as the Internet.[139] This feat requires a global effort and is distinct from the typical disclosure of information.[140]

Indeed, NITs and TOR are not the only technological advancements presenting privacy concerns within the third-party doctrine. In *United States v. De L'Isle*,[141] the Eighth Circuit addressed the reasonable expectation of privacy in a user's credit card information under the third-party doctrine.[142] Under a rigid application of the third-party doctrine, consumers lose all reasonable expectation of privacy in their bank account when they swipe to make a purchase.[143] Cellphone location tracking has also prompted privacy concerns.[144] Moreover, the Eleventh Circuit expressed a deep concern over third-party doctrine enabling the government to intrude on vast amounts of personal information, even when users take several steps to conceal that information:

> [T]he majority's blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment. Consider the information that Google gets from users of its e-mail and online search functions. . . .

---

which routes communications through multiple computers called 'nodes' in order to mask a user's IP address and, thus, keeps the user's identity anonymous.").

139. *See* Scharr, *supra* note 137 (explaining how a data packet passing through the TOR network is not fully traceable).

140. *See id.* ("[U]nlike the case with normal Internet connections, Tor strips away part of the packet's header, which is a part of the addressing information that could be used to learn things about the sender such as the operating system from which the message was sent.").

141. United States v. De L'Isle, 825 F.3d 426 (8th Cir. 2016).

142. *See id.* at 432 ("When the holder uses the card[,] he 'knowingly disclose[s] the information on the magnetic strip of his credit card to a third party and cannot claim a reasonable expectation of privacy in it.'" (quoting United States v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *11 (S.D. Fla. Oct. 24, 2009))).

143. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 442 (9th Cir. 2016) (maintaining the idea that voluntary conveyance of information to a third party diminishes one's expectation of privacy in the information).

144. *See* Recent Case, *Fourth Amendment – Warrantless Searches – New Jersey Supreme Court Holds that State Constitution Requires Police to Obtain Warrant Before Accessing Cell-Site Location Information.* – State v. Earls, *70 A.3d 630 (N.J. 2013)*, 127 HARV. L. REV. 2164, 2164 (2014) (footnotes omitted) ("Lower federal courts and state courts, the early battlegrounds on which privacy disputes are waged, are often hesitant to distinguish Supreme Court precedent, even when changes in the technological landscape are dramatic. A conflict of this nature has been brewing in the courts over whether law enforcement must obtain a warrant before accessing individuals' cell-site location information (CSLI) from cell phone service providers."); *see generally* Shannon Jaeckel, Comment, *Cell Phone Location Tracking: Reforming the Standard to Reflect Modern Privacy Expectations*, 77 LA. L. REV. 143 (2016) (discussing Louisiana's laws regarding cell site location information and competing privacy interests).

> Google collects information about you (name, e-mail address, telephone number, and credit card data); the things you do online (what videos you watch, what websites you access, and how you view and interact with advertisements); the devices you use (which particular phone or computer you are searching on); and your actual location. . . . Under a plain reading of the majority's rule . . . we give up any privacy interest in that information.[145]

Thus, there is strong support for the proposition that the third-party doctrine, in its current form, is insufficient for addressing TOR or other digital issues, which will undoubtedly arise as society continues to advance. This is not a novel proposition. In *United States v. Jones*,[146] Justice Sotomayor warned the third-party doctrine may require change as society modernizes:

> More fundamentally, it 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 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . 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.[147]

---

145. United States v. Davis, 785 F.3d 498, 535–36 (11th Cir. 2015) (Martin, J., dissenting) (footnotes omitted). The court continued:

> And why stop there? Nearly every website collects information about what we do when we visit. So now, under the majority's rule, the Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we "friend," or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask "cloud"-based file-sharing services like Dropbox or Apple's iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this. But as far as I can tell, every argument the government makes in its brief regarding cell site location data applies equally well to e-mail accounts, search-engine histories, shopping-site purchases, [and] cloud-storage files . . . .

Id. at 536; *see also Mohamud*, 843 F.3d at 442 (explaining that conveyance of information to a third party diminishes a privacy interest, even if disseminated in confidence).

146. United States v. Jones, 565 U.S. 400 (2012).

147. *Id.* at 417–18 (Sotomayor, J., concurring).

Courts at all levels, from all parts of the country, have recognized the possible futility of the third-party doctrine in a digital age.[148] And until the

148. *See* United States v. Wheelock, 772 F.3d 825, 829 (8th Cir. 2014) (recognizing "the Supreme Court may revise its view on third-party disclosures in the digital context, but until then, we are bound by precedent, and the actual majority opinion in *Jones* did not address the third-party disclosure doctrine, let alone purport to desert or limit it"); *see also In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 623 (5th Cir. 2013) (Dennis, J., dissenting) ("Justice Sotomayor cast the critical fifth vote in support of the majority opinion. However, her concurrence expressed serious doubt about extending the third party records doctrine applied in [*Smith*] and relied upon by today's majority . . . ."); Apodaca v. N.M. Adult Prob. and Parole, 998 F. Supp. 2d 1160, 1180 (D.N.M. 2014) (stating "it may no longer be sound to universally hold to the third-party disclosure rule to determine whether a subjective expectation of privacy exists"); New York v. Thompson, 28 N.Y.S.3d 237, 250 (N.Y. 2016) ("The [third-party] doctrine has also been subject to significant criticism[.]"). The *Thompson* court goes on to quote Justice Sotomayor, adopting her reasoning that it may be necessary to reconsider the premise underlying the third-party doctrine, because it 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." *Id.* at 251 (quoting *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring)). Further, the court explains how in a modern society, it is common for people to "relay sensitive personal information by email," and that it would be archaic to preclude Fourth Amendment protection because of the third-party doctrine. *See id.* ("[T]he assertion that no Fourth Amendment protections apply to such communications because email requires an email account, in this Court's view, is an archaic notion which negates the protection of the Fourth Amendment for many of our most private communications."); *see also* Commonwealth v. Augustine, 4 N.E.3d 846, 863 n.35 (Mass. 2014) ("Although, as stated in the text, we do not reject the third-party doctrine as a general matter, the rapid expansion in the quantity of third-party data generated through new technologies raises important questions about the continued viability of the third-party doctrine in the digital age."); Tracey v. Florida, 152 So. 3d 504, 519 (Fla. 2014) (agreeing "it might be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (citing *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring))). Of importance is Justice Sotomayor's belief that the third-party doctrine is not apt in a digital age, where people are comfortable revealing personal information about themselves on a daily basis, and through the course of routine tasks. *See id.* at 519–20 (citing *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring)) (describing Justice Sotomayor's thoughts on the way people share information); *see also* Wisconsin v. Tate, 849 N.W.2d 798, 828 (Wis. 2014) (Abrahamson, C.J., dissenting) ("Justice Sotomayor got it right in her concurrence in [*Jones*], which casts doubt on the continued viability of a broad third-party doctrine in the digital age[.]" (citing *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring))); Ford v. Texas, 444 S.W.3d 171, 202 (Tex. App.—San Antonio 2014, pet. granted) (Chapa, J., dissenting) ("But the Supreme Court has recently recognized that modern cell phones—now a 'pervasive and insistent' part of modern life—present privacy concerns far beyond the founding principles of the Fourth Amendment and the circumstances of the founding era." (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014))). The *Ford* court reasoned that just as cellphones altered Fourth Amendment jurisprudence, modern society has advanced to the point that mundane tasks involve conveying information to third parties, and so the law should again adjust. *See id.* at 202 ("Similar to the way that the search-incident-to-arrest doctrine was ill suited to the digital data contained on cell phones seized during an arrest, the third-party doctrine 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.'" (quoting *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring))).

Supreme Court re-examines the issue,[149] courts across the country will continue to produce differing opinions.

From a logical approach, the third-party doctrine is surely outdated. It is difficult to imagine that an expectation of privacy is rendered void if the information is conveyed to the Central Intelligence Agency through sophisticated and confidential communication channels. On a less sophisticated scale, it is also rejected that an expectation of privacy is void merely because the information was communicated to an attorney to gain legal advice, or to a doctor to obtain treatment. If placing a "No Trespassing" sign is not enough to obtain a reasonable expectation of privacy,[150] then more than a mere conveyance should be required to nullify a similar expectation of privacy.

A. *A Proposal*

This Comment urges for Supreme Court guidance on the third-party doctrine in the digital age. Specifically, the Court must create a framework which considers the *nature* of a conveyance to a third-party and requires a detailed examination of the *circumstances* surrounding a disclosure. To illustrate the importance, consider whether society should prevent innocent people from using TOR, or whether the focus should only be on criminals. Remaining anonymous is not necessarily criminal. Some users have legitimate legal reasons to utilize TOR.[151] The Eleventh Circuit recognized

---

149. *See* United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016) (en banc) (acknowledging the need for the Supreme Court to revisit the third-party doctrine). The court in *Graham* articulated:

> Ultimately, of course, the Supreme Court may decide to revisit the third-party doctrine. Justice Sotomayor has suggested that the doctrine 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." . . . But Justice Sotomayor also made clear that tailoring the Fourth Amendment to "the digital age" would require the Supreme Court itself to "reconsider" the third-party doctrine.
>
> . . . [U]nless and until the Supreme Court so holds, we are bound by the contours of the third-party doctrine as articulated by the Court.

Id. at 437 (quoting *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring)).

150. *See* Oliver v. United States, 466 U.S. 170, 170 (1984) (rejecting the proposition that a "No Trespassing" sign altered Fourth Amendment analysis).

151. *See Criminal Activity and Your IP Address*, ASSOCIATE'S MIND, http://associatesmind.com/2011/08/26/criminal-activity-and-your-ip-address [https://perma.cc/K8RT-QJL7] (enumerating potentially innocent people, such as libertarians or social activists, that may seek to obscure their identity for legitimate reasons when they go online).

the negative consequences of stripping innocent users of their privacy through the third-party doctrine merely because they participated in mundane activities.[152]

But the dynamics change when TOR is used to conduct criminal activity.[153] Criminal activity should be weighed through a balancing test, utilized by a court. This would not be a departure from current law. For instance, the Third Circuit has held a defendant's expectation of privacy is not one society is ready to accept when it is an "unauthorized" transmission.[154] Likewise, the Third Circuit reasoned that an unauthorized driver of a rented vehicle lacked a reasonable expectation of privacy in the vehicle because he is deceiving the true owner.[155] The Supreme Court has

152. *See* United States v. Davis, 785 F.3d 498, 535 (11th Cir. 2015) (Martin, J., dissenting) (arguing against a "blunt application of the third-party doctrine [because it] threatens . . . a staggering amount of private information").

153. *See Peeling the Onion—Tor's Criminal Content Revealed*, INFOSECURITY MAG. (Mar. 2, 2014), http://www.infosecurity-magazine.com/news/peeling-the-onion-tors-criminal-content-revealed [https://perma.cc/Y2AV-5B72] ("The Tor Network has long been known for hosting a large number of resources carrying out illegal activity."); *see also* Cara McGoogan, *Dark web browser Tor is overwhelmingly used for crime, says study*, THE TELEGRAPH (Feb. 2, 2016, 2:35PM), http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study [https://perma.cc/8Y2Z-JU9P] ("In the first study of its kind, researchers at King's College London found that 57 per cent of the sites designed for Tor—known as .onion sites—facilitate criminal activity, including drugs, illicit finance, and extreme pornography."); Sara Peters, *Darknet is Full of Criminals & Governments Giving TOR a Bad Name*, DARK READING (Sept. 15, 2015, 8:00 PM), http://www.darkreading.com/analytics/darknet-is-full-of-criminals-and-governments-giving-tor-a-bad-name/d/d-id/1322211 [https://perma.cc/VR9W-MU9S] ("[TOR contains] a wide assortment of criminal marketplaces – for human trafficking, child pornography, and murder."); *Criminal Activity and Your IP Address*, *supra* note 151 ("Of course, using TOR is also useful if you are attempting to disguise online criminal activity. By routing traffic through a TOR relay, a criminal can 'hide their tracks' to some extent. If law enforcement associates an IP address with the criminal activity on a TOR network . . . they have not found the criminal, but merely the last used TOR exit relay."). *But see* Jack Smith IV, *Stop Calling Tor 'The Web Browser For Criminals'*, OBSERVER (Sept. 16, 2014, 10:33 AM), http://observer.com/2014/09/stop-calling-tor-the-web-browser-for-criminals/ [https://perma.cc/E9V4-CKXP] ("[B]eyond the scary-sounding dark net, there are dozens of use-cases for Tor that have nothing to do with cybercrime."). On balance, however, it is unlikely these "dozens" of legitimate uses outweigh the need to unveil the identity of criminals. *See* Bill Bosen, *Dark Web—Tor Use is 50% Criminal Activity—How to Detect It*, FORTSCALE (May 25, 2016), https://insider.fortscale.com/dark-web-tor-use-is-50-criminal-activity-how-to-detect-it/ [https://perma.cc/P6W2-NZNY\] ("[A]lthough not all Tor usage is cybercriminals, a huge percentage of it is.").

154. *See* United States v. Stanley, 753 F.3d 114, 120–21 (3d Cir. 2014) (rejecting a reasonable expectation of privacy in unauthorized transmissions of child pornography).

155. *See* United States v. Kennedy, 638 F.3d 159, 165 (3d Cir. 2011) (holding an unauthorized driver of a rental car has no reasonable expectation of privacy because he "acts in contravention of the owner's property rights, [and] also deceives the owner of the vehicle").

also chimed in, explaining that even though a burglar robbing a cabin "may have a . . . justified subjective expectation of privacy," society is not ready to accept that expectation as reasonable because a burglar's presence is "wrongful."[156] Therefore, whether a person is committing a crime is certainly a factor in ascertaining whether that person holds a reasonable expectation of privacy.

But, consider this: in the digital age, it might be unreasonable to believe your computer is immune from hacking.[157] Computer hacking has become so common that software experts are providing the public with tips and tricks for avoiding hackers.[158] One expert produced a laundry list of common hacking techniques, including a keylogger, denial of service, waterhole attacks, fake WAPs, eavesdropping, phishing, viruses, trojans, clickjacking attacks, cookie theft, and a bait and switch.[159] Therefore, whether a person is engaged in activity that is prone to hacking could be factored into the equation. The uncertainty, and the need for a balancing inquiry, re-affirms the need to examine the *nature* of a third-party disclosure when assessing a Fourth Amendment interest. However, without revisiting the doctrine, district courts across the country are left holding valid, but outdated law in one hand, and new technological problems in the other.

VIII. CONCLUSION

On one hand, society wants the government to prevent criminals from utilizing TOR. On the other hand, the need for truth and justice may not

156. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (quoting Jones v. United States, 362 U.S. 257, 267 (1960)).

157. *See, e.g.*, Lee Rainie, *How Americans Balance Privacy Concerns with Sharing Personal Information: 5 Key Findings*, PEW RESEARCH CTR. (Jan. 14, 2016), http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/ [https://perma.cc/8EVM-YF2Y] (reporting that members of a focus group "worried about hackers," though some accept privacy tradeoffs as "part of modern life"); *see also* United States v. Matish, 193 F. Supp. 3d 585, 619 (E.D. Va. 2016) ("Now, it seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the internet can—and eventually will—be hacked.").

158. *See, e.g.*, Shritam Bhowmick, *10 Most Popular Ways Hackers Hack Your Website*, DEFENCELY (June 14, 2013), https://defencely.com/blog/10-popular-ways-hackers-hack-website/ [https://perma.cc/ZN6Y-3VVW] (enumerating the ten most popular ways hackers "can threaten the security of your site, and your business" and providing warning signs).

159. *See* Amar Shekhar, *Top 10 Common Hacking Techniques You Should Know About*, FOSSBYTES (June 4, 2016), https://fossbytes.com/hacking-techniques/ [https://perma.cc/9386-LFSG] (providing a cursory exposition of common hacking techniques).

outweigh society's need for privacy.[160] Nevertheless, a thorough examination of the circumstances should be *required.* A static approach to the exclusionary rule is directly at odds to long standing interpretations of the Constitution.[161] Justice Brandeis reasoned that the Constitution is enacted "from an experience of evils," but the Fourth Amendment's language should not be "confined to the form that the evil ha[s] theretofore taken."[162] Constitutional interpretations are not static. It has long been held that as technology advances the law must adjust.[163] This continues to hold true today.

160. *See* United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, slip op. at *7 (W.D. Mo. Oct. 20, 2016) (speaking to whether a user's "subjective desire to maintain his Internet anonymity is one society is prepared to accept as reasonable" the court explains "society as a whole does not believe that patrons and promoters of child pornography should be free to traipse around the Internet like some invisible Peeping Tom"; however, "society might well accept that there are other instances and situations where cyber-anonymity is both important and reasonable"). Indeed, there are instances users utilize TOR for non-criminal activity. *See Criminal Activity and Your IP Address, supra* note 151 (giving examples of persons who may legitimately seek internet anonymity).

161. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting) (indicating constitutional provisions affording protections to individuals "must have a . . . capacity of adaptation to a changing world."), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

162. *Id.*

163. *See, e.g.*, United States v. Davis, 785 F.3d 498, 538 (11th Cir. 2015) (Martin, J., dissenting) (demonstrating "the extent of information" exposed "to third parties has increased" with magnitude since the Supreme Court established the third-party doctrine). Specifically, the *Davis* court explains that when the third-party doctrine was established, nearly forty years ago, it was long before cellphone tracking or the Internet came into existence. *Id.* In light of "extraordinary technological advances," the dissenting judge felt the Supreme Court required lower courts to "critically evaluate how far to extend the third-party doctrine." *Id.* The court also explained how a blanket application of the third-party doctrine would result in a slippery slope, framing the issue as a "perfect example of why the Supreme Court has insisted that technological change sometimes requires us to consider the scope of decades-old Fourth Amendment rules." *Id.* at 537 (citing Kyllo v. United States, 533 U.S. 27, 35 (2001)); *Kyllo*, 533 U.S. at 35 (rejecting a "mechanical interpretation of the Fourth Amendment" in the face of "advancing technology"); *cf. Katz*, 389 U.S. at 353 (recognizing prior Court decisions involving the trespass doctrine and its physical intrusion component have become "so eroded" over time that they "can no longer be regarded as controlling"). A familiar example is *Riley v. California*, 134 S. Ct. 2473 (2014). There, the Court departed from decades-old law because of rapid technological advancements. *See Riley*, 134 S. Ct. at 2484 (finding a departure from old precedent necessary because "phones are based on technology nearly inconceivable just a few decades ago").