St. Mary's Law Journal

Volume 52 | Number 1 Article 5

4-2021

Bitcoin Searches and Preserving the Third-Party Doctrine

Christine A. Cortez
St. Mary's University School of Law

COMMENT

BITCOIN SEARCHES AND PRESERVING THE THIRD-PARTY DOCTRINE

CHRISTINE A. CORTEZ*

* J.D. Candidate 2021, St. Mary's University School of Law; BBA & MPAcc, Texas A&M International University. The author wishes to express her immense gratitude to her parents, Oscar and Lupita Cortez, and her siblings, James, Leslie, & Oscar Jr., for their unconditional love, support, and encouragement throughout all of her endeavors. She is thankful for her family and friends for believing in her and instilling in her the value of hard work. The author would also like to thank members of Volume 52 of the *St. Mary's Law Journal* for their diligent edits in preparing the Comment for publication.

I. INTRODUCTION

Technology is rapidly evolving. Are our current laws still relevant or keeping up with this evolution? This Comment will explore how technology has affected Fourth Amendment jurisprudence, specifically as it relates to digital currency such as bitcoin. As technology evolves, so do the methods criminals use to commit crimes. In the last ten years, bitcoin has caught the attention of criminals who appreciate the supposed anonymity it provides.[1]

Current case law allows government agents to search digital devices using warrants, which appear to lack particularity.[2] In the last decade, the Supreme Court has acknowledged how case law involving the Fourth Amendment may not be sufficient to handle searches in a digital age.[3] While criminals are becoming more sophisticated, the Supreme Court has taken a significant step in protecting people against unreasonable searches and seizures related to electronic devices where bitcoins are stored.[4]

There is nothing inherently wrong with using bitcoin.[5] However, considering its prominence in the dark web, courts should exercise care when adding more stringent requirements to digital searches. There are two competing interests: a person's expectation of privacy and the government's interest in obtaining evidence against criminals who use bitcoin to engage in crimes. Considering recent Fourth Amendment case law changes, I argue how the third-party doctrine allows the government to investigate bitcoin crimes while enabling it to obtain the necessary information to meet the Fourth Amendment's warrant requirements.

Part II of this comment briefly provides information about what bitcoin is, how to get it, how to store it, and its prevalence in crimes. Part III gives a general overview of the Fourth Amendment. Part IV discusses how the Fourth Amendment applies to bitcoin and how obtaining a search warrant

1. Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 1, 7 (2014) (providing reasons why criminals prefer digital currencies such as bitcoin).

2. *See, e.g.*, Riley v. California, 573 U.S. 373, 401 (2014) (requiring a warrant to search the digital contents of a cell phone).

3. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (expressing concern the third-party doctrine is unsuitable in a digital age).

4. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (declining to extend the third-party doctrine to cell phone location records held by cell phone providers); *Riley*, 573 U.S. at 401 (requiring a warrant to search a cell phone even when seized incident to arrest).

5. *See generally Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq [https://perma.cc/9JG4-6UJA] (listing legitimate advantages of using bitcoin over traditional currencies).

of bitcoin wallets may be problematic, considering how the Supreme Court recognizes and creates case law that affords digital devices greater privacy protections. Considering this trend, Part IV analyzes how these changes may make it difficult for government agents to meet the Fourth Amendment's probable cause and particularity requirements for a search warrant. Part IV explores the legality of a government agent's ability to review Bitcoin's public ledgers for potential criminal offenses and whether a warrant is needed to search certain bitcoin information made public in light of the third-party doctrine.

Part V discusses how new case law limiting the third-party doctrine is inapplicable to certain Bitcoin searches and concludes with the need to maintain the third-party doctrine.

II. THE RISE OF DIGITAL CURRENCY

A. *What Is Bitcoin?*

Bitcoin is a form of digital currency used in exchange for goods and services.[6] It is a digital payment system where people pay using digital money, similar to people shopping online using a credit card.[7] Unlike most national currencies, no government or single administrator controls bitcoin.[8] Bitcoin is also not available in a printed form like other national currencies such as the U.S. dollar.[9] Bitcoins are entirely digital, represented by a unique sequence of numbers and letters, and created using free computer software.[10] People analogize bitcoin mining to mining for gold.[11] Bitcoins are created by miners who use computers to solve complex mathematical puzzles, which help create a bitcoin transaction record.[12] Their reward for solving the problems and adding to the record is a newly

6. *Id.*

7. *See What Is Bitcoin?*, COINDESK (Jan. 26, 2018), https://www.coindesk.com/information/what-is-bitcoin [https://perma.cc/85MK-GH76] (explaining bitcoin can be used to pay for goods or services electronically wherever bitcoin is accepted as a payment).

8. *Id.*

9. *Id.*

10. *Id.*; John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCIENCE (Mar. 9, 2016, 9:00 AM), https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin [https://perma.cc/XX6R-DSQZ].

11. *How Bitcoin Mining Works*, COINDESK (Jan. 26, 2018), https://www.coindesk.com/information/how-bitcoin-mining-works [https://perma.cc/5PQV-AEPK]; *Frequently Asked Questions*, *supra* note 5.

12. *How Bitcoin Mining Works*, *supra* note 11.

issued bitcoin.[13] Also, unlike how the Federal Reserve regulates the production of new dollars, the Bitcoin system is set up only to create a total of 21 million bitcoins.[14]

B. *How Bitcoin Began*

Bitcoin is the original type of cryptocurrency that uses cryptography to secure its system.[15] An unknown person, going by the pseudonym Satoshi Nakamoto, developed Bitcoin in 2008.[16] They described it as a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[17] The idea of cryptocurrency is that all Bitcoin users may control it using mathematical calculations, and it eliminates the need to go through intermediaries.[18] Nakamoto believed the current method of processing electronic payments through financial institutions using what he describes as a "trust-based model" has inherent weaknesses, such as human error and fraud.[19] Nakamoto's most significant concerns with using intermediaries are that (1) they cannot effectively deal with fraud and (2) financial transactions are reversible, which is a disadvantage to merchants.[20] He proposed Bitcoin as a solution to his concerns, a system based on cryptographic proof rather than trust, shifting trust from financial institutions and people to math and technology.[21] Just as bitcoin miners mine to create bitcoins, miners earn bitcoins for solving mathematical

13. *Id.*

14. *Frequently Asked Questions*, *supra* note 5; Luke Fortney, *Bitcoin Mining, Explained*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bitcoin-mining.asp [https://perma.cc/Q3ZK-W4PQ].

15. Jake Frankenfield, *Cryptocurrency*, INVESTOPEDIA, https://www.investopedia.com/terms/c/cryptocurrency.asp [https://perma.cc/6AQ2-6F7E]. The meaning of the prefix crypto is "concealed or secret." Shobhit Seth, *Explaining the Crypto in Cryptocurrency*, INVESTOPEDIA, https://www.investopedia.com/tech/explaining-crypto-cryptocurrency [https://perma.cc/HZR9-53FH]. (defining the prefix crypto and explaining "[c]ryptography is the mathematical and computational practice of encoding and decoding data").

16. *What Is Bitcoin?*, *supra* note 7 (stating no one knows Nakamoto's true identity).

17. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/2N2L-R99T].

18. *Frequently Asked Questions*, *supra* note 5.

19. Nakamoto, *supra* note 17, at 1.

20. *See id.* (commenting on how merchants have to be cautious of customers and fear the risk of having their transactions reversed due to fraud).

21. *Id.*

equations that verify the bitcoin used in the transaction is not duplicated, which prevents buyers from double-spending.[22]

C. *Storing and Acquiring Bitcoin*

Before owning a bitcoin, users have to decide where they will save them.[23] This storage is known as a "wallet."[24] Users have various storage options available: they may use their computer, cell phone, hardware such as a portable hard drive, or paper.[25] The advantages of installing a software wallet on a computer are that it is usually free, easy to set up, and allows users to have control over their keys.[26] Unfortunately, users must be careful because hackers may have access to users' wallets and bitcoins if hackers gain access to their computers.[27] Users may also use cloud wallets, which allows users access to their bitcoins from any device.[28] While cloud wallets are convenient, this storage method also offers lower security because users are entrusting a third party to secure their money.[29] Mobile wallets allow users to access their bitcoins from their mobile devices.[30] Some users prefer using hardware wallets to store their bitcoins because they are usually offline, making them more secure and difficult to hack.[31] The disadvantage of using a hardware wallet or storing your bitcoin on a portable hard drive is that, if the device is lost or stolen, you may lose those bitcoins too.[32] Another option for bitcoin users is to write down their bitcoin keys on paper.[33] While paper is not hackable, it is easier to lose or destroy.[34]

After users create a digital wallet, they may begin acquiring bitcoins. People can acquire bitcoins by accepting them "[a]s payment for goods and services," purchasing bitcoins from a specialized exchange such as Bitfinex,

22. Although mathematics is used to solve problems, most of mining is a guessing game. Miners use computers to solve the problems and many miners work together, combining computing power to solve the equations faster. Fortney, *supra* note 14.

23. *How to Store Your Bitcoin*, COINDESK (Jan. 26, 2018), https://www.coindesk.com/information/how-to-store-your-bitcoins [https://perma.cc/ZUE7-ZC7F].

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

Coinbase, Bitstamp, or Poloniez, exchanging bitcoins with other bitcoin users, or bitcoin mining.[35] After acquiring bitcoin, users are issued a public and private key that may be stored in the digital wallet.[36] Users share their public key—similar to an email address—with other users to transfer bitcoins.[37] Users use their private key—similar to a debit card PIN—to authorize transactions.[38]

Unlike cash transactions, Bitcoin records every transaction on a public ledger known as a blockchain.[39] Everyone has access to the blockchain.[40] Users can use the blockchain to verify the authenticity of a bitcoin payment and ensure the payment is coming from the bitcoin's rightful owner.[41]

There are several advantages of using bitcoin instead of traditional currencies, the first being that it allows for payment freedom.[42] People do not have to worry about bank holidays, borders, or bureaucracy,[43] allowing users can exchange bitcoins at any time from any place in the world.[44] Merchants benefit from accepting bitcoins because the transactions are irreversible,[45] and Bitcoin provides merchants better protection against fraud.[46] Buyers benefit from using bitcoin because there is stronger protection against identity theft, and buyers do not have to worry about erroneous merchant charges.[47] Another advantage is that all bitcoin transactions are available on a public ledger for users to verify transactions.[48] Also, bitcoin transactions and accounts are not linked to real-world identities unless the user provides personal information.[49] While

35. *Frequently Asked Questions*, *supra* note 5; *How Can I Buy Bitcoin?*, COINDESK, https://www.coindesk.com/information/how-can-i-buy-bitcoins [https://perma.cc/PVT2-GCJX].

36. *How Do Bitcoin Transactions Work?*, COINDESK, https://www.coindesk.com/information/how-do-bitcoin-transactions-work [https://perma.cc/3WYG-DMCF].

37. Prableen Bajpai, *How to Buy Bitcoin*, INVESTOPEDIA, https://www.investopedia.com/tech/how-to-buy-bitcoin [https://perma.cc/ZB4J-KELK].

38. *Id.*

39. *How Does Bitcoin Work?*, BITCOIN, https://bitcoin.org/en/how-it-works [https://perma.cc/76XC-Q6ND].

40. *Id.*

41. *Id.*

42. *Frequently Asked Questions*, *supra* note 5.

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

48. *How Does Bitcoin Work?*, *supra* note 39.

49. *Frequently Asked Questions*, *supra* note 5.

most people use bitcoin for legal purposes, criminals take advantage of bitcoin's anonymity to engage in illegal activities.[50]

D. *Criminal Activity Involving Bitcoin*

There is nothing inherently wrong with using bitcoin to transact with others. Bitcoin provides legitimate benefits to individuals, businesses, and organizations because it minimizes the risk of fraud by preventing double-spending or duplicating money.[51] This benefit attracts criminals because it reduces the risk of getting scammed.[52] Another advantage is business transactions may occur without tying a person's personal information, which helps prevent identity theft.[53] Because of this, there is a perception bitcoin allows for anonymity, which further attracts criminals.[54] There are thousands of cryptocurrencies, but bitcoin is the original and most common form of cryptocurrency used in crimes involving cryptocurrency.[55] Criminals use bitcoin for trafficking illegal goods, soliciting child pornography, tax evasion, money laundering, funding terrorism, "and even murder for hire."[56]

One of the best examples of using bitcoin for illegal purposes is the story of a black-market website known as Silk Road.[57] Silk Road started as a marketplace for people to buy and sell drugs.[58] As such, people commonly referred to Silk Road as the "[a]mazon.com" for drugs.[59] Buyers and sellers used bitcoin exclusively because of its perceived anonymity.[60] Using bitcoin and other encryption tools allowed users to engage in illegal activity without

50. *What Is Bitcoin?*, *supra* note 7.

51. Nikita Malik, *How Criminals and Terrorists Use Cryptocurrency: And How To Stop It*, FORBES (Aug. 31, 2018, 10:08 AM), https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#2cf57f763990 [https://perma.cc/T29F-7AVB].

52. *Id.*

53. *Frequently Asked Questions*, *supra* note 5.

54. Malik, *supra* note 51.

55. Jen Wieczner, *Bitcoin Accounts for 95% of Cryptocurrency Crimes, Says Analyst,* FORTUNE (Apr. 24, 2019), https://fortune.com/2019/04/24/bitcoin-cryptocurrency-crime [https://perma.cc/E9AR-GLXX].

56. Stephen Small, Comment, *Bitcoin: The Napster of Currency*, 37 HOUS. J. INT'L L. 581, 583 (2015) (describing how bitcoin is used for illegal purposes).

57. *See* Larry McIntyre, Comment, *Cyber-Takings: The War on Crime Moves into the Cloud*, 14 PITT. J. TECH. L. & POL'Y 333, 342–43 (2014) (discussing the origins of Silk Road).

58. *Id.* at 342–43.

59. *Id.* at 342.

60. *Id.* at 343.

the fear of getting caught.[61] It took two years for the government to find the website owner, and that was only because the owner inadvertently exposed his identity.[62] In the last few years, more cases involving Bitcoin have emerged, and in almost every case, the defendant argued the government violated the Fourth Amendment.[63]

III. FOURTH AMENDMENT OVERVIEW

The United States Constitution's Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[64]

Nevertheless, the Fourth Amendment does not guarantee absolute protection against all searches—only unreasonable ones.[65] Historically, the Fourth Amendment's protection was limited to physical intrusions into constitutionally protected areas such as homes.[66] Early interpretation of the Fourth Amendment required a "trespass" analysis.[67] Since *Katz v. United States*,[68] cases involving the Fourth Amendment have adopted Justice Harlan's reasonable expectation of privacy analysis.[69] *Katz* introduced the notion the Fourth Amendment protects people and not places,[70] and this analysis predominated for decades.[71] Nevertheless, the trespass analysis is still alive.[72] In recent years, the Court has, on occasion,

61. *What Is Bitcoin?*, *supra* note 7.

62. McIntyre, *supra* note 57, at 343.

63. *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 98 (2d Cir. 2017) (arguing the government violated the defendant's privacy interest by monitoring his IP address traffic).

64. U.S. CONST. amend. IV.

65. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) ("For 'what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.'" (quoting Elkins v. United States, 364 U.S. 206, 222 (1960))).

66. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) (concluding the Fourth Amendment was not violated when the government tapped a person's telephone conversations because there was no physical trespass onto his property), *overruled by* Katz v. United States, 389 U.S. 347, 352–53 (1967).

67. *See Olmstead*, 277 U.S. at 465–66 (exemplifying a trespass analysis).

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

69. United States v. Jones, 565 U.S. 400, 406 (2012).

70. *Katz*, 389 U.S. at 353.

71. *Jones*, 565 U.S. at 406.

72. *Id.* at 406–07.

relied on a trespass analysis.[73] Thus, the government can implicate a person's Fourth Amendment right in two ways: (1) a search by a governmental agent of an area where a person has a reasonable expectation of privacy; or (2) a physical trespass into a constitutionally protected area such as a home.[74]

To determine whether a person has a reasonable expectation of privacy under the Fourth Amendment, courts use a subjective and objective test.[75] The defendant must establish an actual, subjective expectation of privacy in the place searched, and the subjective expectation must be one society would accept as reasonable.[76] If the person has a reasonable expectation of privacy, a police officer needs a warrant to search the area unless the search satisfies one of the warrant requirement exceptions.[77] A neutral and detached magistrate judge issues the warrant after the officer has proven probable cause.[78] If there is no trespass or reasonable expectation of privacy, then a search warrant is not needed.

Generally, the Fourth Amendment does not protect information a person shares with third parties.[79] A person does not have a reasonable expectation of privacy for information he shares with others.[80] The general rule is if someone provides information to a third party, that person does not have a reasonable expectation of privacy, and a government agent may obtain that information from third parties without a warrant.[81] This belief is true even if someone believed the information shared with a third party would remain private.[82] In *Hoffa v. United States*,[83] the Supreme Court held the Fourth Amendment does not protect information shared with others because of a person's "misplaced belief that a person to whom he voluntarily

73. *Id.* at 404–05.

74. *See id.* at 406–07 (holding the Fourth Amendment protects against government trespass); *see also Katz*, 389 U.S. at 353 (explaining the reach of the Fourth Amendment cannot turn solely on the presence or absence of a physical intrusion into any given enclosed structure).

75. *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

76. *Id.*

77. *Id.* at 361–62.

78. United States v. Ventresca, 380 U.S. 102, 109–10 (1965).

79. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–44 (1976).

80. *See* United States v. Dionisio, 410 U.S. 1, 14 (1973) (explaining there is not a reasonable expectation of privacy in the sound of one's voice).

81. *Miller*, 425 U.S. at 445–46 (concluding Defendant did not have a Fourth Amendment interest to dispute the subpoena of his bank records).

82. *Id.* at 443.

83. Hoffa v. United States, 385 U.S. 293 (1966).

confides" will not share that information with someone else.[84] This idea is one of the concepts behind the third-party doctrine.[85]

The consequence of not having the third-party doctrine is that if a government agent successfully obtained evidence against a defendant through an unlawful search, such evidence might be subject to the exclusionary rule. The exclusionary rule prevents the government from presenting evidence obtained through an unlawful search.[86] Its purpose is to deter government agents from violating a person's Fourth Amendment right by conducting an unlawful search.[87] Stricter laws may hinder the government's ability to find criminals or obtain evidence. If a court deems the government's search unlawful, it is possible the government is prevented from presenting such crucial evidence.[88]

IV. APPLYING THE FOURTH AMENDMENT TO BITCOIN

Bitcoin searches can occur in at least three different ways.[89] A government agent can search a person's digital wallet,[90] the Bitcoin public ledger,[91] or subpoena records from third-party exchanges who assist in the buying, selling, and managing of cryptocurrency. The Fourth Amendment is implicated differently in each scenario.

84. *Id.* at 302.

85. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."); *Miller*, 425 U.S. at 440 (stating a person's Fourth Amendment rights are not implicated unless the government has intruded into one's "zone of privacy" and information shared with third parties is not private).

86. *See* Mapp v. Ohio, 367 U.S. 643, 656 (1961) (stating the exclusionary rule is "an essential part of the right to privacy" the Fourth Amendment is trying to protect); Weeks v. United States, 232 U.S. 383, 391–92 (1914) (explaining those who execute the criminal laws to obtain conviction by means of unlawful search and seizures "should find no sanction in the judgment of the courts").

87. United States v. Calandra, 414 U.S. 338, 347 (1974) ("[T]he [exclusionary] rule's prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures.").

88. United States v. Ulbricht, 858 F.3d 71, 94 (2d Cir. 2017).

89. Will Yakowicz, *Startups Helping the FBI Catch Bitcoin Criminals*, INC. (Jan. 9, 2018), https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html [https://perma.cc/3RBF-YJEC].

90. *Ulbricht*, 858 F.3d at 100–01 (explaining how a search warrant may be used to search a hard drive for bitcoin wallet files).

91. *See* Yakowicz, *supra* note 89 (discussing how startup companies are helping law enforcement by creating forensic software which identifies patterns in detecting crimes and tracing the transactions to the end user).

A. *Searching Bitcoin Wallets and the Limitations of Cell Phones*

Bitcoin raises several Fourth Amendment search issues because of how people obtain and store the cryptocurrency.[92] Federal courts have issued opinions that demonstrate a trend toward affording more protection to the information contained in electronic devices.[93] As technology evolves, courts are slowly beginning to adapt to that change. The nature of modern technology, which holds so much data and personal information, has caused the courts to think more broadly about what a protected interest is and more narrowly about the third-party doctrine exception.[94]

For example, the Court—applying *Katz*—has long permitted officers to search persons incident to a lawful arrest so that they may protect themselves or preserve evidence of the crime.[95] Nevertheless, the Supreme Court recognized the need to adapt to the advancement of technology, especially as it relates to storage, surveillance, and communication.[96] In *Chimel v. California*,[97] the Supreme Court held when an officer arrests a person, the officer may search the person incident to a lawful arrest without a warrant to protect themselves or preserve evidence of a crime.[98] Forty-

92. *See* Jonathan Lane, Note, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 540 (2014) ("As applied to Bitcoin, perhaps the most important Fourth Amendment issue is law enforcement's ability to search and/or seize the digital currency and the personal computers and devices used for its storage and transfer.").

93. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (acknowledging how gaining access to a person's cell phone location allows the government to take a peek into the intimate details of a person's life); Riley v. California, 573 U.S. 373, 403 (2014) (holding a warrant is needed to search data information on a cell phone seized from an arrestee due to the privacy concerns implicated because of the immense amount of information contained inside them); United States v. Blood, 429 F. App'x 670, 671 (9th Cir. 2011) ("A laptop computer is entitled to the same Fourth Amendment protection as other closed containers and personal effects."); Lane, *supra* note 92 (finding a "trend in federal court rulings suggest[ing]" electronic devices are afforded the same Fourth Amendment protection as containers).

94. *See Carpenter*, 138 S. Ct. at 2214 ("This sort of digital data—personal [cellphone-cite] location information maintained by a third party—does not fit neatly under existing precedents.").

95. *See, e.g.*, Chimel v. California, 395 U.S. 752, 762–63 (1969) ("[I]t is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.").

96. *See Carpenter*, 138 S. Ct. at 2214 (recognizing the importance of preserving a person's Fourth Amendment right to privacy against the government as technology evolves); Kyllo v. United States, 533 U.S. 27, 34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

97. Chimel v. California, 395 U.S. 752 (1969).

98. *Id.* at 762–63.

five years later, the Supreme Court limited the holding by requiring government agents to obtain a warrant before searching a cell phone.[99]

In *Riley v. California*,[100] the Court ruled that officers may only examine a cell phone's physical characteristics with a search warrant, but not the information contained inside it.[101] The Court reasoned that such a search implicates significant privacy concerns.[102] While cell phones are like any container that might contain evidence of a crime, they pose a special danger compared to other containers, such as a cigarette pack, where you may find evidence of a crime, or a bag, which may contain a weapon.[103] The term "cell phone" is misleading because cell phones are more than just containers or devices used to text and talk.[104] Cell phones are essentially minicomputers, which "could easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[105] Before cell phones came around, people were not carrying every piece of personal information around with them.[106] Today, law enforcement can retrace a person's life based on photos, texts, search, and location history contained in a phone.[107] While current Supreme Court cases involve the use of cell phone searches and their privacy concerns, the same privacy concerns apply to computers because of their "immense storage capacity," GPS capability, and Internet access.[108]

Most people store bitcoins in electronic devices such as cell phones, computers, the cloud, or offline storage devices. Because of the vast amount of information contained in these types of electronic devices, searching these devices for bitcoin information can be problematic. Computers, cell phones, and digital storage devices include more than just a bitcoin digital wallet; they hold a significant amount of private information, implicating

99. Riley v. California, 573 U.S. 373, 403 (2014).

100. Riley v. California, 573 U.S. 373 (2014).

101. *Id.* at 387.

102. *Id.* at 394.

103. *See* United States v. Robinson, 414 U.S. 218, 221–23 (1973) (describing an instance where an officer pulled over a person for driving with a revoked license, arrested him, searched his pocket, and found a cigarette pack which contained capsules of heroin).

104. *Riley*, 573 U.S. at 393.

105. *Id.*

106. *Id.* at 395.

107. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218, 2220 (2018) (explaining how the government can use historical cell-site location information to retrace a person's every move).

108. *See Riley*, 573 U.S. at 393–94 (analogizing cell phones to minicomputers and discussing how the ability to store an immense amount of data in a single device brings forward privacy issues that searches of other physical items do not).

privacy concerns grounded in the Fourth Amendment.[109] Because of these concerns, coupled with the ease of getting a warrant, a warrant is required in most cases before searching through a digital device's contents.

A valid search warrant must meet three requirements. First, the issuing magistrate must be detached and neutral.[110] Second, the warrant must be based on probable cause using a totality of the circumstances analysis with information provided to the magistrate judge by a government agent.[111] Third, the warrant must describe the property or place to be searched with particularity.[112]

Establishing probable cause to search digital storage devices for bitcoin evidence is problematic.[113] Considering how long it takes for government agents to decipher bitcoin information, it may be difficult for the agents to develop probable cause before someone transfers the bitcoins elsewhere.[114] When issuing a warrant, a "magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."[115] Analytical tools allow government agents to find suspicious patterns within the Bitcoin blockchain.[116] Although agents may see the transactions and the associated Bitcoin public addresses used in the exchange, discovering the identity of the owner is difficult because agents lack the IP address needed to trace the transaction back to the person or digital device.[117] The Bitcoin system is designed to hide IP addresses from their corresponding transactions.[118] The challenge with establishing probable cause is that bitcoins may change hands instantaneously.[119] Thus, by the time the government identifies a user, the bitcoin investigated may no longer belong to that user. This makes it difficult for the government agent to prove probable cause.[120]

109. *Id.* at 393.
110. Johnson v. United States, 333 U.S. 10, 13–14 (1948).
111. Illinois v. Gates, 462 U.S. 213, 230–31 (1983).
112. Marron v. United States, 275 U.S. 192, 196 (1927).
113. Lane, *supra* note 92, at 540–43.
114. *Id.*
115. *Gates*, 462 U.S. at 238.
116. Yakowicz, *supra* note 89.
117. Bohannon, *supra* note 10.
118. *Id.*
119. Lane, *supra* note 92, at 542.
120. *Id.*

Obtaining a warrant to search a cell phone, computer, or cloud storage may also prove to be somewhat challenging because of the particularity requirement. The particularity requirement to obtain a warrant is a significant safeguard against unreasonable search and seizure; it prevents the government from having the ability to obtain a general warrant to search without limitation.[121] The framers of the U.S. Constitution deliberately inserted the particularity safeguard in response to the abuse of warrants in England against the colonists, which allowed English officers to search at will.[122] The prevention of general searches is not the only purpose of the particularity requirement.[123] The particularity requirement also lets an individual know that an officer's search is lawful, indicates what is being seized, and states the scope of the search.[124] Warrants protect people's right to privacy.

A warrant must meet three requirements to adhere to the particularity requirement of the Fourth Amendment. First, the warrant must list the specific offense the government agent believes they have probable cause for.[125] Second, a warrant must describe "the place to be searched."[126] Third, the warrant must describe "the persons or things to be seized."[127]

Because of the amount of information in electronic devices containing bitcoin wallets, it may be challenging to meet the particularity requirement.[128] Digital device searches are significantly different from searches of other physical items.[129] Unlike a search of physical evidence such as a purse or drawers, a search for information contained in an

121. *See* Payton v. New York, 445 U.S. 573, 583–85 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

122. *Id.* at 608 (White, J., dissenting).

123. Groh v. Ramirez, 540 U.S. 551, 561 (2004).

124. *See* United States v. Chadwick, 433 U.S. 1, 9 (1977) (citing Camara v. Mun. Ct. of City & Cnty. of San Francisco, 387 U.S. 523, 532 (1967)).

125. U.S. CONST. amend. IV.

126. *Id.*

127. *Id.*

128. *See* United States v. Ulbricht, 858 F.3d 71, 101–02 (2d Cir. 2017) (illustrating how the defendant deliberately hid files using labels such as "mbsobzvkhwx4hmjt" which makes it difficult for government agents to find using key words or cursorily reviews).

129. Riley v. California, 573 U.S. 373, 393 (2014) ("Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person.").

electronic device usually requires an officer to take the entire device offsite to review the information inside.[130]

Despite the concerns about warrants meeting the particularity requirement, courts continue to allow government agents to search electronic devices even when the warrant only describes the device, type of device, or place where the device may be found.[131] The current case law on digital searches is "deferential to law enforcement."[132] The Federal Rules of Criminal Procedure recognize the need for government agents to seize computers and take them offsite to search, as searching onsite is impracticable for law enforcement agents.[133]

For example, in *United States v. Ulbricht*,[134] the Second Circuit investigated the issue regarding whether the use of a warrant to search a laptop for evidence relating to the dark web website, Silk Road, and the resulting bitcoin wallet transactions met the particularity requirement.[135] The defendant argued the warrant to search and seize his laptop "violated the Fourth Amendment's particularity requirement."[136] The Second Circuit acknowledged how a search of a computer hard drive provides government agents with a trove of sensitive information.[137] The court went further to admit: "Where . . . the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance."[138] Legal scholars and courts analogize computer hard drives to residences because of the amount of private information contained inside.[139] Notwithstanding this acknowledgment, the Second Circuit held the search for bitcoin evidence in a laptop was lawful because a warrant does not need to describe

130. James T. Stinsman, Comment, *Computer Seizures and Searches: Rethinking the Applicability of the Plain View Doctrine*, 83 TEMP. L. REV. 1097, 1102 (2011); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1, 6 (2015).

131. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 214–15 (2018).

132. Kerr, *supra* note 130, at 6.

133. FED. R. CRIM. P. 41(e)(2)(B); Kerr, *supra* note 130, at 6.

134. United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).

135. *See id.* (explaining the Fourth Amendment's particularity requirement related to warrants to search technology).

136. *Id.* at 99.

137. *Id.*

138. *Id.* (quoting United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013)).

139. *See Galpin*, 720 F.3d at 446 ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.").

the items searched perfectly.[140] The court reasoned a broad warrant does not automatically mean the warrant lacks particularity.[141]

The current case law seems to allow government agents to obtain broad warrants to search through digital devices, "so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant."[142] In light of *Carpenter v. United States*[143] and *Riley* (which are not warrant cases), it seems that deference to government agents may diminish.[144] Even in *Ulbricht*, the Second Circuit conceded that a different case than the one in front of them might require them to add limitations to digital searches to ensure warrants for digital searches meet the Fourth Amendment's particularity requirement.[145]

Some courts are urging judges to examine search warrants of digital devices more carefully.[146] In *People v. Covlin*,[147] the New York Supreme Court found two warrants to search through digital devices lacked particularity.[148] The New York Supreme Court found one warrant lacked particularity because it allowed law enforcement to search the defendant's home for any type of electronic or paper record without limitation.[149] The court found the other warrant lacked particularity because it granted the

140. *Ulbricht*, 858 F.3d at 100.

141. *Id.*

142. *Id.* (internal quotation marks omitted) (quoting *Galpin*, 720 F.3d at 446).

143. Carpenter v. United States, 138 S. Ct. 2206 (2018).

144. *See id.* at 2218 (illustrating how cell phone technology has changed decades old case law relating to searches); Riley v. California, 573 U.S. 373, 393–94 (2014) (describing how cell phones implicate greater privacy concerns than other physical searches). *Carpenter* and *Riley* are not specifically about what is required when a warrant is obtained; however, their reasoning may lead courts to impose stricter requirements on officers seeking warrants.

145. *Ulbricht*, 858 F.3d at 104.

146. *See* People v. Covlin, 70 N.Y.S.3d 342, 347 (N.Y. Sup. Ct. 2018) (emphasizing the importance of courts affording proper deference to the process, so as not to defeat search warrants); Alyssa C. Goldrich, *A Step in the Right Direction: Judge Suppresses Evidence Seized in Murder Case Due to Overbroad Computer Search Warrants*, GDB LAW (Feb. 5, 2018), https://www.gdblaw.com/overboard-computer-search-warrants [https://perma.cc/BR6S-EGTG] ("[U]ntil the law can catch up to rapid technological innovations in society, search warrants seeking to access a defendants digital data must be scrutinized with the utmost diligence in order to effectively preserve one's Constitutional right to be free from unreasonable searches and seizures.").

147. *Covlin*, 70 N.Y.S.3d at 347–49.

148. *Id.*

149. *Id.* at 347–48.

search of a cell phone for any stored electronic information.[150] While this is a major win for advocates of protecting privacy, it is particularly worrisome for government agents who need access to a person's digital and paper records to find bitcoin transactions. Again, bitcoin keys can be stored digitally inside physical storage devices, the cloud, or on paper.

Bitcoin storage wallets, like other digital evidence, differ substantially from other forms of physical evidence.[151] While it is true that digital storage devices contain an immense amount of private information, it is also true that government agents will not always know where bitcoin information is stored. Criminals may conceal bitcoin information within a large volume of other digital information, essentially making the bitcoin information a needle in a haystack. Unfortunately, this means searching for evidence relating to bitcoin may inevitably lead to sorting through irrelevant private information. Because a warrant allows the agent to search the entire wallet in its investigation of a single bitcoin, anything the government finds in that wallet could be fair game through the "plain view" doctrine.[152] The plain view doctrine is an exception to the general rule requiring a warrant to search objects.[153] The Supreme Court reasons "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."[154]

A recent case from a Michigan district court involving bitcoin helps illustrate this issue. In *United States v. Stetkiw*,[155] Homeland Security Investigations was initially investigating Stetkiw for violations related to

150. *Id.* at 348–49.

151. *See* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 57–58 (2018) (differentiating digital evidence from other forms of evidence because digital data is easier to conceal than other physical evidence, which can be hidden away in physical areas or containers).

152. *See* Horton v. California, 496 U.S. 128, 135–37 (1990) (holding government agents may conduct a warrantless seizure as long as they are lawfully on the premises, discover evidence of a crime that is in plain view, and have probable cause to believe the property is evidence of a crime); Arizona v. Hicks, 480 U.S. 321, 323–26 (1987) (explaining how the plain view doctrine was inapplicable when a police officer, while investigating a shooting inside an apartment, moved two stereos to see their serial numbers because he had a reasonable suspicion the stereos were stolen, but lacked the necessary probable cause); Yuval Simchi-Levi, *Search Warrants in the Digital Age*, 47 HOFSTRA L. REV. 995, 1005 (2019) (discussing how the majority of circuit courts hold the plain view doctrine is applicable to electronic evidence as long the search for digital evidence is reasonably needed based on what is in the search warrant).

153. *Horton*, 496 U.S. at 133.

154. *Id.* (citing *Hicks*, 480 U.S. at 325).

155. United States v. Stetkiw, No. 18-20579, 2019 WL 2866516 (E.D. Mich. July 3, 2019).

running an unlicensed bitcoin exchange service.[156] The government had a warrant to search through Stetkiw's computer data and image files.[157] While searching through the image files, the government agent found child pornography.[158] After discovering the image, the agent immediately stopped the search and obtained another search warrant for child pornography and subsequently found more images.[159]

Stetkiw's attorneys then filed a motion to suppress the child pornography evidence found while searching the computer for bitcoin evidence.[160] His lawyers argued the search warrant lacked particularity, and a search of computer images was unrelated to uncovering bitcoin evidence.[161] The court held the warrant was particular because it identified all forms of storage, including images, and the agent who searched the computer justified the search of pictures because people may hide bitcoin information in various locations inside the computer.[162] The government agent who searched the computer also testified he needed to look through the image files for bitcoin evidence because the image files may contain bitcoin QR codes, the information needed to recover a bitcoin wallet, and wallet passwords.[163]

The court denied the motion to suppress the evidence because the agent had probable cause to search the computer image files for bitcoin evidence, and the child pornography photo was in plain view.[164] Before concluding the opinion, the judge expressed concern about the agent's testimony during the evidentiary hearing regarding the computer search.[165] The agent stated, "[t]here were no practical limitations to what could be searched for on Stetkiw's computer."[166] To the judge, this statement sounded like a general warrant.[167] Nevertheless, while the judge ruled the search constitutional, they recommend that for the future, the magistrate judge issuing a warrant should conduct an *ex ante* review of the search procedures to assist courts

156. *Id.* at *1.
157. *Id.*
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.* at *2.
163. *Id.*
164. *Id.* at *3–4.
165. *Id.* at *4.
166. *Id.*
167. *Id.*

and agents in conducting searches that do not violate the Fourth Amendment.[168]

The *Stetkiw* case demonstrated how a computer search allowed the government to discover evidence against "the bad guys." But what about the good guys? While this is a win for the government agents combating crime and protecting society against people who illegally possess child pornography, this example is not illustrative of every potential circumstance. Would innocent people feel comfortable with a government agent searching through their private photos? What if the images of child pornography did not belong to Stetkiw but someone else instead? What if someone planted the images inside the computer through a virus?[169] These questions are probably far-fetched ideas in Stetkiw's case but could be a viable defense in other circumstances. The level of anonymity bitcoin provides makes it difficult for agents to know where exactly bitcoin is stored and who it belongs to, which requires government agents to have some reasonable flexibility in conducting searches.

In the last decade, the Supreme Court has issued three significant opinions relating to searches of digital storage devices.[170] These cases demonstrate the Court is now seriously confronting the applicability of Fourth Amendment case law in a more technological society. They also demonstrate how the Court is imposing significant limitations on searches and prioritizing the people's right to privacy. Considering this trend, it appears as though the Court or Congress may impose a stricter particularity requirement. With this in mind, we must find other avenues in which government agents can obtain bitcoin evidence to combat crimes without violating a person's right to privacy.

168. *Id.* at *4–5.

169. *See generally* Simchi-Levi, supra note 152, at 1002 (explaining how the Second Circuit held government agents may require a search of an entire electronic device to refute a defendant's claim that a hacker placed files into a person's computer thorough a hacking or virus).

170. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (exemplifying how technology affects third-party doctrine caselaw); Riley v. California, 573 U.S. 373, 403 (2014) (holding a warrant is needed to search data information on a cell phone seized from an arrestee because a cell phone is not a weapon and people have reasonable expectation that the information contained in their cell phones is private); United States v. Jones, 565 U.S. 400, 404–05 (2012) (ruling the government must obtain a warrant before installing a GPS device on someone's vehicle because monitoring a vehicle's every move is a search).

B. *Bitcoin's Public Ledger and a Person's Reasonable Expectation of Privacy*

Government agents may have better luck searching and analyzing Bitcoin's blockchain because people do not have a reasonable expectation of privacy to information provided directly and indirectly on Bitcoin's blockchain. Generally, the Fourth Amendment does not protect information a person knowingly shares with the public.[171] The Fourth Amendment only protects against unreasonable searches when a person has a reasonable expectation of privacy of the information or place searched.[172] Courts apply a two-part inquiry to determine whether an expectation of privacy is reasonable.[173] Courts first assess whether a person subjectively believes that she has an expectation of privacy.[174] Secondly, courts evaluate whether society would objectively recognize the expectation of privacy as reasonable.[175] A person's expectation of privacy must also be legitimate.[176] A legitimate expectation of privacy does not mean that a person had a subjective belief she would not be discovered.[177]

The first step in determining whether a person has a reasonable expectation of privacy is to assess whether a person has a subjective expectation of privacy when he uses bitcoin, knowing the transaction is displayed permanently in Bitcoin's blockchain. There are several reasons why a person should not have a subjective expectation of privacy.

Satoshi Nakamoto describes bitcoin as a "peer-to-peer version of electronic cash," which allows people to send an electronic payment to other parties without having an intermediary such as a bank facilitating the process.[178] To prevent people from double-spending bitcoin, miners use computers to solve mathematical problems that confirm the authenticity of the transactions and record the transactions onto a permanent record

171. Katz v. United States, 389 U.S. 347, 351 (1967).

172. Byrd v. United States, 138 S. Ct. 1518, 1526 (2018); *Jones*, 565 U.S. at 406; United States v. Miller, 425 U.S. 435, 442 (1976); *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

173. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

174. *Id.*

175. *Id.*

176. Rakas v. Illinois, 439 U.S. 128, 143 (1978).

177. *See id.* at 143 n.12 ("A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'").

178. Nakamoto, *supra* note 17.

known as the blockchain or public ledger.[179] As a reward for honest work, the system creates new bitcoin and issues bitcoins to the miners.[180]

Everyone who has Internet access may search and see the bitcoin public ledger at any time.[181] There is a record of every Bitcoin transaction on the Bitcoin blockchain. The blockchain is named as such because each digital transaction is one of several transactions contained inside a "block."[182] Miners then record each block on the "chain," which is its shared public ledger.[183] Each transaction tells viewers the time, date, amount spent, and address involved in the transaction.[184] What the block might not tell you is the identity of the person who sent or received the bitcoin.[185] Thus, people are under the misconception that bitcoin is entirely anonymous, keeping their transactions free from unauthorized intrusion.[186] This perception is not accurate. Bitcoin's website acknowledges the misperception of it being an anonymous payment system.[187] Bitcoin prides itself as being "the most transparent payment . . . in the world."[188] Bitcoin is inherently not private because it is information a person knowingly shares with the public.[189]

Satoshi Nakamoto discussed privacy in his bitcoin paper and explained how traditional banking systems could provide a certain level of privacy by limiting the amount of information provided to other parties. Bitcoin, on the other hand, does not allow for this level of privacy because of the necessity to record all transactions on the blockchain to help people verify the authenticity of each bitcoin transaction.[190] Nakamoto does address how a certain level of privacy can be achieved by "keeping public keys

179. *Id.*

180. *Id.*

181. I—a person who does not own any bitcoin—did a quick google search for "Bitcoin Blockchain" and was directed to a website that shows me the bitcoin and ethereum, another form of cryptocurrency, blockchain. Fortney, *supra* note 14.

182. *Id.*

183. *Id.*

184. *Id.*

185. Bohannon, *supra* note 10.

186. *Id.* ("'It's totally anonymous,' was how one commenter put it in Bitcoin's forums in June 2013. 'The FBI does not have a prayer of a chance of finding out who is who.'").

187. *Protect Your Privacy*, BITCOIN, https://bitcoin.org/en/protect-your-privacy [https://perma.cc/TG3T-DDDA].

188. *Id.*

189. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

190. Nakamoto, *supra* note 17, at 6.

anonymous."[191] Bitcoin's website explicitly states that all of its transactions are "public, traceable, and permanently stored in the Bitcoin network."[192] The website also acknowledges once someone uses a bitcoin, it is forever "tainted by the history of all transactions ever involved with."[193] Further, Bitcoin also recognizes how someone may trace a bitcoin address to a specific user and encourages users to take precautions in protecting their privacy.[194]

These facts suggest there is no reasonable expectation of privacy because of the very idea the blockchain contains a public record of all bitcoin transactions that anyone with an Internet connection can access without accessing the individual's computer.[195] The core of Bitcoin's infrastructure requires a permanent and public record so that others may verify the authenticity of the transactions.[196] While a person's real name might not appear on the blockchain, there are other methods in which others can link a person to a specific bitcoin.[197] For example, if a person exchanges his bitcoin address in-person to a merchant who accepts bitcoins as a payment, the merchant now knows the individual's real identity.[198]

Moreover, people should not have a reasonable expectation of privacy since Bitcoin warns its users of the ability for someone "to listen for transactions' relays and log their IP addresses."[199] Most federal circuit courts hold a person does not have a reasonable subjective expectation of privacy for IP address information.[200] IP addresses may reveal a person's

191. *Id.*

192. *Protect Your Privacy*, *supra* note 187.

193. *Id.*

194. *Id.* ("As the block chain is permanent, it's important to note that something not traceable currently may become trivial to trace in the future.").

195. *See* Eric Wall, *Privacy and Cryptocurrency, Part I: How Private is Bitcoin?*, MEDIUM (Mar. 7, 2019), https://medium.com/human-rights-foundation-hrf/privacy-and-cryptocurrency-part-i-how-private-is-bitcoin-e3a4071f8fff [https://perma.cc/A3DU-P49P] (explaining Bitcoin is only semi-private).

196. Nakamoto, *supra* note 17, at 2 (explaining how the only way the system can prevent others from double-spending bitcoins is by requiring all Bitcoin transactions are publicly recorded).

197. Wall, *supra* note 195.

198. *Id.*

199. *Protect Your Privacy*, *supra* note 187.

200. *See* United States v. Ulbricht, 858 F.3d 71, 97–98 (2d Cir. 2017) (joining other circuit courts in holding a warrant is not required to for the government to collect IP addresses because a person does not have a "legitimate privacy interest" in IP address information); United States v. Wheelock, 772 F.3d 825, 828–29 (8th Cir. 2014) ("Wheelock cannot claim a reasonable 'expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.'" (alteration in original) (quoting United States v. Suing, 712 F.3d 1209,

location and Internet Service Provider (ISP), which in turn may reveal a person's identity.[201] There are even geolocation IP databases that allow you to determine a person's approximate location using his IP address.[202] People may expose their identities even when connected to another person's Wi-Fi network or a public Wi-Fi network because of the person's browser history or stored cookies on a personal computer.[203]

Furthermore, even if a person believes he has a reasonable expectation of privacy for information made public on the blockchain, it is not one society may accept or recognize as a reasonable expectation of privacy. Bitcoin is a "decentralized peer-to-peer payment network that is powered by its users."[204] The very nature of Bitcoin's peer-to-peer network and structure requires that transactions are public,[205] which leaves "extensive public records."[206] Regarding peer-to-peer networks, a person who makes a "decision to install and use file-sharing software [on his computer]," which opens "his computer to anyone else with the same freely available program," does not have a reasonable expectation of privacy.[207] The same conclusion applies to a person's expectation of privacy concerning bitcoin transactions because a person who knowingly and voluntarily uses bitcoin as a payment method cannot expect information that is recorded permanently on the blockchain, for others to see and verify, to be private.[208] Bitcoin's

1213 (8th Cir. 2013))); United States v. Christie, 624 F.3d 558, 573–74 (3d Cir. 2010) (holding an expectation of privacy of IP address information is unreasonable (citing United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008))); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (analogizing Internet users to telephone users, stating neither has a reasonable expectation of privacy because Internet users know their "IP addresses are not merely passively conveyed through third party equipment" and are instead "voluntarily turned over" to ISPs to direct the communication).

201. Wall, *supra* note 195.

202. *Id.* (providing an example of a website which provides a rough approximate location of a user using an IP address); *Inception*, TOR, https://2019.www.torproject.org/about/torusers.html.en [https://perma.cc/HSC3-REMA] (stating how mapping a person's location using an IP address is becoming increasingly precise).

203. Wall, *supra* note 195 (providing an example of how a person's Dropbox application will associate a person's account with the IP address used whenever connected to the Internet as soon as the laptop is turned on).

204. *Frequently Asked Questions*, *supra* note 5.

205. *Protect Your Privacy*, *supra* note 187.

206. *Frequently Asked Questions*, *supra* note 5.

207. United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008).

208. *See* United States v. Weast, 811 F.3d 743, 747–48 (5th Cir. 2016) (holding a person does not have an expectation of privacy when he "widely and voluntarily" disseminates information through the ordinary use of peer-to-peer software); *Ganoe*, 538 F.3d at 1127 (describing a case where a government agent did not violate the Fourth Amendment when he used LimeWire, a peer-to-peer

blockchain is not a peer-to-peer software where users share files, but it is a peer-to-peer network where other users confirm other user transactions.

On the other hand, a person may argue he has a reasonable expectation of privacy of his identity because there is a difference between a permanent record of a bitcoin transaction and a record of his identity. While a person may recognize his transactions are logged permanently on the blockchain public ledger, he may still maintain the subjective expectation that this identity or IP addresses would remain concealed because bitcoin information on the blockchain does not contain personally identifiable information. Some users take extra precaution by utilizing tools to hide their identity or IP address.[209] In *Katz*, the Supreme Court held the Fourth Amendment does not protect information a person knowingly shares with the public.[210] However, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[211] In *Katz*, the Court held that a defendant did not lose his Fourth Amendment protection merely because he used a public telephone booth.[212] By closing the telephone booth door, the defendant expected his telephone conversation was private.[213]

While many bitcoin users might not take steps in protecting their privacy, some sophisticated users deliberately try and protect their personal information.[214] Like in *Katz*, if people take precautions in preventing exposure of their real-life identity by using tools that mask their IP addresses, people should not lose their expectation of privacy merely because their transaction is public.[215] Bitcoin encourages users to protect their privacy by informing them only to use a specific bitcoin address once, not sharing their addresses, and using tools that make tracing IP addresses

software, to access a defendant's computer to find child pornography files because the defendant did not have a reasonable expectation of privacy when he used the software).

209. United States v. Brown, 857 F.3d 334, 337 (6th Cir. 2017) (describing how Tor, a tool used to mask one's IP address, "routes online communications through anonymizing proxy computers" to conceal the user's true identity).

210. Katz v. United States, 389 U.S. 347, 351 (1967).

211. *Id.*

212. *Id.* at 152 ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

213. *Id.*

214. *See* United States v. Ulbricht, 858 F.3d 71, 82 (2d Cir. 2017) (illustrating how Ulbricht used Tor, a tool used to make it difficult for people to trace Internet traffic).

215. *See Katz*, 389 U.S. at 352 ("But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").

difficult.[216] Under current case law, any attempt a person may make to conceal IP address information is possibly futile because a person cannot expect privacy when it comes to IP address information.[217]

For example, bitcoin users use a popular tool to mask a person's IP address: Tor.[218] Tor is a free software used to block third-party trackers from accessing a person's Internet cookies, guard against other people who try and monitor someone's Internet usage, and provide Internet data traffic encryption.[219] Despite using this tool, many courts hold there is still no reasonable expectation of privacy in protecting one's IP address.[220] In *United States v. Matish*,[221] the court found a person's subjective expectation of privacy is not objectively reasonable because Tor requires Internet users to provide their real IP address.[222] By providing his IP address to a third party, the Tor user lost his expectation of privacy.[223] For some courts, this finding is seemingly limited to the collection of IP addresses and does not allow government agents to access the contents of one's computer without a warrant.[224] Nevertheless, if the government can discover an IP address without searching unlawfully through a person's computer, there is no reasonable expectation of privacy.

Moreover, the government does not violate a person's Fourth Amendment rights when an agent uses computer software to perform a

216. *Protect Your Privacy*, *supra* note 187.

217. *See Ulbricht*, 858 F.3d at 97–98 (holding collecting IP addresses is not protected by the Fourth Amendment, even when using tools such as Tor to conceal identities).

218. David Hollerith, *Bitcoin Is Not Anonymous and Tor Users Are Forgetting This*, BITCOIN MAG. (Sept. 20, 2019), https://bitcoinmagazine.com/articles/bitcoin-is-not-anonymous-and-tor-users-are-forgetting-this [https://perma.cc/4G2Z-T6RP]; *see also* Andy Greenberg, *The Grand Tor: How To Go Anonymous Online*, WIRED (Dec. 9, 2017, 6:00 AM), https://www.wired.com/story/the-grand-tor [https://perma.cc/67HP-HDXW] (indicating how millions of Internet users utilize Tor for the closest thing to anonymity on the Internet).

219. *Tor: Overview*, TOR, https://2019.www.torproject.org/about/overview.html.en [https://perma.cc/BB2V-35FX]; Greenberg, *supra* note 218.

220. United States v. Matish, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016) ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address.").

221. United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016).

222. *Id.* at 616–17.

223. *Id.*

224. *See* United States v. Ulbricht, 858 F.3d 71, 97–98 (2d Cir. 2017) (limiting the holding to the collection of IP addresses and stating a warrant was not required because the government did not access the defendant's communications).

forensic analysis of bitcoin's blockchain.[225] While one may analogize the government using computer software to analyze the blockchain to law enforcement officers handling a thermal imaging device from outside a person's home to detect heat within the house, the reliance on that analogy is misplaced because both concepts are fundamentally different.[226] In *Kyllo v. United States*,[227] government agents suspected the defendant was growing marijuana inside his home.[228] The agents scanned the exterior of the defendant's home using a thermal imager to detect radiation consistent with the use of high-intensity lamps for growing marijuana indoors.[229] Justice Scalia, writing for the majority, stated: "[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[230]

The difference between the facts in *Kyllo* and the government's use of computer software to analyze the blockchain is that in the former, the government is using technology not available to the general public to get a peek inside a person's home, a constitutionally protected area.[231] The Supreme Court has long recognized a person's home is afforded the greatest Fourth Amendment protection because it is one's "most private space."[232] A home is an area that society as a whole would deem private because "[a]t the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[233] Nevertheless,

225. *See* United States v. Norman, 448 F. App'x 895, 896 (11th Cir. 2011) (per curiam) (rejecting defendant's claim that law enforcement violated the Fourth Amendment by using a specialized software to view contents of a computer folder everyone in the peer-to-peer network had access to). *See generally Ulbricht*, 858 F.3d at 98 (holding the government did not violate the Fourth Amendment by using pen registers to trap and trace IP addresses).

226. *See Norman*, 448 F. App'x at 896 (distinguishing a home from information shared with others in a peer-to-peer network); *Ulbricht*, 858 F.3d at 98 (contrasting software used to monitor a person's "IP address traffic through his router" which is not protected by the Fourth Amendment to a thermal imager used from outside a person's home, which is protected by the Fourth Amendment).

227. Kyllo v. United States, 533 U.S. 27 (2001).

228. *Id.* at 29.

229. *Id.* at 30.

230. *Id.* at 34 (citation omitted) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

231. *See* U.S. CONST. amend. IV (providing people have a right against "unreasonable searches and seizures" inside their homes); *see also Kyllo*, 533 U.S. at 40 (acknowledging a person's home is a constitutionally protected area).

232. Kentucky v. King, 563 U.S. 452, 474–75 (2011) (Ginsburg, J., dissenting).

233. Silverman v. United States, 365 U.S. 505, 511 (1961) (citing Boyd v. United States, 116 U.S. 616, 626–30 (1886)).

with regard to Bitcoin, the government is not using technology to take a glimpse into one's most private space. The government uses technology to analyze Bitcoin's public ledger, which is not constitutionally protected because it is shared publicly on the Internet.[234]

By recognizing that people do not have a reasonable expectation of privacy for information available, directly and indirectly, through the Bitcoin blockchain and IP address information, the Bitcoin blockchain further enables government agents to crack down on crimes using cryptocurrencies such as bitcoin. The government can trace blockchain and IP address information without accessing an individual's computer, which lessens the likelihood of rummaging around in personal information. The government's ability to analyze data and track IP addresses gives it a better chance of obtaining information needed to establish probable cause to meet the Fourth Amendment's search warrant requirements. Changing this part of the caselaw may adversely affect government agents from effectively investigating crimes involving bitcoin, especially if the Legislature or courts decide to impose stricter warrant requirements.

C. *Applying the Third-Party Doctrine to Bitcoin*

Currently, government agents may obtain bitcoin evidence through third parties.[235] The Supreme Court established this third-party doctrine in *United States v. Miller*[236] and *Smith v. Maryland*.[237] In *Miller*, the Alcohol, Tobacco, and Firearms Bureau (ATF) requested financial records from banks holding the defendant's financial accounts.[238] The banks complied with the request.[239] The defendant moved to suppress the bank records from being presented as evidence at trial.[240] The Court held that the Fourth Amendment does not protect the bank records because they are part of the

234. *See* United States v. Norman, 448 F. App'x 895, 897 (11th Cir. 2011) (per curiam) (finding the defendant did not have a reasonable expectation of privacy for information shared from the defendant's computer because it was available through a peer-to-peer network); *cf.* United States v. Dionisio, 410 U.S. 1, 14 (1973) (stating there is no reasonable expectation of privacy in a voice recording because a "voice is repeatedly produced for others to hear").

235. *See* United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (asserting there is a general consensus amongst federal courts indicating a person's Fourth Amendment rights are not violated when ISPs provide subscriber information to the government).

236. United States v. Miller, 425 U.S. 435 (1976).

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

238. *Miller*, 425 U.S. at 437–38.

239. *Id.* at 438.

240. *Id.*

bank's commercial records.[241] The documents were not Miller's private papers.[242] The Supreme Court stated:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. 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.[243]

In *Smith v. Maryland*, a telephone company installed a pen register after police, without a warrant, requested it to do so after a robbery victim began receiving threatening phone calls from the alleged robber.[244] The pen register successfully identified the caller, and the defendant moved to suppress any information obtained through the use of the pen register.[245] The Supreme Court held the use of the pen register did not violate the Fourth Amendment because a person does not have a reasonable expectation of privacy in a number dialed on the telephone.[246] The Court reasoned there is no reasonable expectation of privacy for this information because all telephone users know the phone numbers dialed are provided to the phone companies to connect the calls.[247] The Court also reasoned there is no reasonable expectation of privacy because telephone users know phone companies maintain a record of the phone calls for billing purposes.[248]

Under current caselaw, subpoenaing third parties to provide information on bitcoin users is possible. Government agents may subpoena ISPs or bitcoin exchanges to provide certain disclosures. There is an old rule that the government may compel others to disclose evidence they have within their possession.[249] While the government does not need to meet the

241. *Id.* at 444.

242. *Id.* at 440–41.

243. *Id.* at 443 (citing United States v. White, 401 U.S. 745–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

244. Smith v. Maryland, 442 U.S. 735, 737 (1979).

245. *Id.* at 735, 737.

246. *Id.* at 742.

247. *Id.*

248. *Id.*

249. Carpenter v. United States, 138 S. Ct. 2206, 2228 (2018) (Kennedy, J., dissenting).

Fourth Amendment's warrant requirements to obtain a subpoena, a subpoena does not carry the same legal force as a warrant in allowing government agents to search and seize.[250] Someone who receives a subpoena may object to the subpoena before complying, which adds a safeguard to assist in mitigating the intrusion.[251]

In Part IV.B, I discussed how most circuit courts agree people do not have a reasonable expectation of privacy for IP address information. Because of the third-party doctrine, government agents may obtain IP address information from ISPs.[252] Similar to how people are associated with telephone numbers or mailing addresses, every device connected to the Internet is associated with a unique address known as an IP address.[253] An IP address is similar to a telephone number because it provides the identity of the IP address's owner; however, it does not reveal the actual contents of the communication.[254] If, while investigating a crime involving bitcoin, a government successfully retrieves an IP address, the government may request IP information from the ISP without a warrant.[255] This concept is true because the person does not have a reasonable expectation of privacy for IP information, and a person knows this IP address information is shared with ISPs so they may "make communication among electronic devices possible."[256] Moreover, Internet users know they use third-party equipment to communicate over the Internet.[257] While one may argue access to this information is an invasion of privacy because it allows for government surveillance, the Supreme Court has not overruled the third-party doctrine as it relates to IP addresses.[258]

Applying the third-party doctrine, the government may obtain bitcoin information by requesting information from bitcoin exchanges. People can buy and sell bitcoins through specialized exchanges such as Bitstamp,

250. *See id.* (explaining the difference between a warrant and a subpoena).

251. *Id.* (citing Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 195 (1946)).

252. *See* cases cited *supra* note 200.

253. United States v. Ulbricht, 858 F.3d 71, 83–84 (2d Cir. 2017).

254. *Id.* at 84; United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

255. *See Ulbricht*, 858 F.3d at 97 (discussing the investigator's ability to obtain IP information from an ISP without a warrant).

256. *Id.*

257. *Id.* at 96.

258. *Id.* at 96–97 (declining to deviate from the third-party doctrine because, in this specific case, the government did not gain access to the actual contents of the computer by collecting IP address information).

Bitfinex, Coinbase, and several others.[259] While specialized exchanges are not banks, they are financial services companies, also known as Money Services Businesses (MSBs), with money transmission licenses that require them to comply with federal laws applicable to financial institutions.[260] Exchanges are considered MSBs that are required to comply with federal regulations because they engage in money transmission services. An MSB engages in money transmission services by accepting "currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[261]

While exchanges are subject to various federal and state money transmission regulations, some of "the most direct and effective regulations relatable to the use of Bitcoin in the criminal enterprise are the federal Bank Secrecy Act (BSA) and anti-money laundering (AML) statutes."[262] The Bank Secrecy Act requires MSBs to verify customer identities, report specific transactions, and retain records for up to five years.[263] The USA Patriot Act goes further to require MSBs to keep exhausted records and maintain information regarding their customers' identities.[264] The purpose of this record keeping is to ensure banks have a system in place to assist law enforcement in deterring and detecting crimes through the misuse of financial institutions.[265]

The reasoning in *Miller* is applicable when dealing with specialized exchanges because *Miller* dealt with records that belonged to banks.[266] Exchanges are not banks in the usual sense, but they are required to maintain records just like banks. As such, people who go through specialized exchanges voluntarily provide their information to exchanges, and the

259. *See* Prableen Bajpai, *A Look at the Most Popular Bitcoin Exchanges*, INVESTOPEDIA (Oct. 16, 2019) https://www.investopedia.com/articles/investing/111914/look-most-popular-bitcoin-exchanges.asp [https://perma.cc/KSQ9-FQZN] (describing various bitcoin exchanges).

260. *Coinbase Money Transmission and E-Money Regulatory Compliance*, COINBASE, https://support.coinbase.com/customer/en/portal/articles/2689172-coinbase-regulatory-compliance [https://perma.cc/8KYP-9RF2] (listing statutes money services businesses must comply with).

261. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2014).

262. Lane, *supra* note 92, at 535 (footnotes omitted).

263. *Coinbase Money Transmission and E-Money Regulatory Compliance*, *supra* note 260.

264. Lane, *supra* note 92, at 536–37 (explaining the requirements of the USA Patriot Act).

265. *Bank Secrecy Act (BSA)*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html [https://perma.cc/589D-UBRT].

266. *See* United States v. Miller, 425 U.S. 435, 445–46 (1976) (concluding defendant did not have a Fourth Amendment interest to dispute the subpoena of his bank records).

government does not violate their Fourth Amendment right just because it obtains information from the exchanges. For example, Coinbase discloses to its customers that they must comply with various regulations, which include verifying their identities and keeping records of it.[267]

V. WHY THE THIRD-PARTY DOCTRINE CONTINUES TO APPLY TO BITCOIN

The Supreme Court decided both *Miller* and *Smith* in the 1970s. To say times have changed would be an understatement. Since the third-party doctrine's inception, the Court has consistently held that the Fourth Amendment does not protect information shared with third parties.[268] The 2018 landmark Supreme Court case *Carpenter v. United States* finally put a restriction on the doctrine.[269] The Court held officers needed a search to obtain historical cell phone location records from cell phone companies.[270] The Court reasoned that cell phones pose a genuine privacy concern because this would allow the government to track everyone's movement.[271] The Court was also careful in stating this was a narrow ruling and did not change the third-party doctrine as it applied to most areas such as bank records.[272] There has been some discussion about reconsidering the third-party doctrine altogether. Justice Sotomayor has expressed that the third-party doctrine is unsuitable in this digital age because of the amount of information people share with third parties during the ordinary course of someone's day.[273]

Since *Carpenter*, many defendants have moved to suppress evidence obtained through third parties such as ISPs or bitcoin exchanges.[274] In *Carpenter*, the Supreme Court's principal concern was with the government's seemingly limitless ability to track a person's every movement through historical cell site location information.[275] The Court was also concerned

267. *Coinbase Money Transmission and E-Money Regulatory Compliance*, *supra* note 260.

268. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216–17, 2220 (2018) (declining to apply the third-party doctrine).

269. *See id.* at 2220 (declining to apply *Smith* and *Miller* and thereby restricting the third-party doctrine).

270. *Id.* at 2221.

271. *Id.* at 2217–18.

272. *Id.* at 2220.

273. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

274. *See* United States v. Kidd, 394 F. Supp. 3d 357, 358 (S.D.N.Y. 2019) (declining to apply Carpenter's holding to IP address information).

275. *Carpenter*, 138 S. Ct. at 2217–18.

with the government's ability to "travel back in time" and track a person's life for the past five years.[276] Cell Site Location Information (CSLI) raises technology concerns that bitcoin does not. Cell phones are almost like an appendage to the human body.[277] People carry their phones with them everywhere they go.[278] The government's access to this information provides more than just their location; this access "provides an intimate window into a person's life."[279]

There are several reasons why IP address information is fundamentally different from CSLI. CSLI allows the government to treat cell phones like GPS monitoring devices and enables the government to see a person's every move for up to five years, depending on the cell phone carrier's retention schedule.[280] Second, cell phones ping location information to the nearest cell phone tower without any voluntary action from the cell phone user.[281] In contrast, an IP address is generated when a person makes the "affirmative decision to access a website or application."[282] Third, while someone can find a person's location using an IP address, an additional process is needed to find the location. When the government acquires the IP address, that address does not contain the location, just numbers.[283] CSLI reveals, "without an independent investigation," the cell phone user's location.[284] So long as IP addresses do not enable the government to track a person's every move, *Carpenter* should not apply.[285] Again, the Supreme Court was concerned with total surveillance.[286] An IP address is like a phone number or address. If the IP address information is used to only find the identity of

276. *Id.* at 2218.

277. *Id.*

278. *See id.* (analogizing a cell phone to an ankle monitor).

279. *Id.* at 2217.

280. *See id.* at 2217–18 (explaining the CSLI allows the government to trace a person's whereabouts and cellphones are comparable to GPS devices); *see also* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (citing *Carpenter* and holding that the CSLI and telephones essentially comprise a GPS system that the government has access to).

281. *Carpenter*, 138 S. Ct. at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes . . . .").

282. *Hood*, 920 F.3d at 92.

283. *Id.*

284. *Id.*

285. *See* United States v. Kidd, 394 F. Supp. 3d 357, 367–68 (S.D.N.Y. 2019) (declining to extend *Carpenter* to IP address information because the defendant failed to prove IP address information enabled the government to track his daily movements).

286. *See Carpenter*, 138 S. Ct. at 2218 (expressing the concern of "near perfect" surveillance).

individuals and does not allow the government to retrieve the actual contents of the communication, then a person does not have a reasonable expectation of privacy for IP address information.

Regarding bitcoin exchanges, fortunately, *Carpenter* did not affect *Miller*'s holding. In *Carpenter*, the Supreme Court explicitly stated its decision does not disrupt *Miller*.[287] The Court deliberately chose not to address "business records that might incidentally reveal location information."[288] While bitcoin exchanges are not financial institutions in the usual sense, the government does not treat them differently from other financial institutions by imposing federal laws such as the Bank Secrecy Act.

VI. CONCLUSION

Despite living in a digital world, the third-party doctrine should be preserved and only limited on a case-by-case basis. The third-party doctrine allows the government to keep up with criminals. Without this legal principle, the government would need to rely on the Legislature to enact laws that assist them in finding criminals. It is imperative to recognize the Supreme Court was deliberate in limiting their holding to CSLI.

Furthermore, with CSLI, the government knows the identity of the person it wants the CSLI from. It makes sense to require a warrant to obtain historical location information because the government should demonstrate they have probable cause in believing a crime was committed or is in the process of being committed. On the other hand, concerning bitcoin, without the third-party doctrine, the government's ability to find a criminal is severely hindered because the government relies on IP information to discover a criminal's identity. Sophisticated criminals find ways to hide their identities, and statutes or caselaw should not restrict the government from using IP address information to assist it in finding them. IP address information allows government agents to find suspects and get the probable cause needed to obtain a warrant. If the Legislature or courts impose stricter warrant requirements in the future, the government's need for IP address information is even greater. If the information is limited to discovering the person's identity behind the IP address, there should not be a strong privacy concern.

While I am concerned IP address information may one day reveal extensive location data similar to CSLI, I also believe we must remember

287. *Id.* at 2220.
288. *Id.* at 2210.

what is at the core of the Fourth Amendment, protection against *unreasonable* searches.[289] Concerning bitcoin, when determining whether the government violated an individual's Fourth Amendment right, courts should assess the government's reasonableness by weighing the government's great interest with the defendant's lessened (or nonexistent) privacy interests.[290] Considering how criminals are using digital currencies to fund crimes and how difficult it is to find a criminal's identity when using bitcoin, it is imperative the third party is preserved and only limited on a case-by-case basis.

289. Terry v. Ohio, 392 U.S. 1, 9 (1968) (citing Elkins v. United States, 364 U.S. 206, 222 (1960)).

290. *See, e.g.*, Maryland v. King, 569 U.S. 435, 461 (2013) ("The reasonableness of any search much be considered in the context of the person's *legitimate* expectations of privacy.") (emphasis added).