Science and Technology Law Review

Volume 24 | Number 1 Article 6

2021

The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy

Daniel Penn
Southern Methodist University, Dedman School of Law

THE FIFTH CIRCUIT, FOURTH AMENDMENT, AND THE THIRD-PARTY DOCTRINE: TWO TAKEAWAYS FROM THE COURT'S FIRST RULING ON BITCOIN PRIVACY

*Daniel Penn**

I. INTRODUCTION

As technology moves into previously uncharted territory, the law must follow closely behind, either by adapting prior decisions to fit the new terrain or establishing new precedent. Virtual currencies, such as Bitcoin, are certainly no exception and present courts with the novel issue of whether users have a reasonable expectation of privacy regarding their Bitcoin transactions worthy of Fourth Amendment protection. In *United States v. Gratkowski*, the Fifth Circuit declined to extend that protection to information stored on the publicly available Bitcoin blockchain, as well as personal information kept by Bitcoin exchanges.[1] Largely basing its decision on the third-party doctrine, the court reasoned that users voluntarily turn over personal information to create accounts on a Bitcoin exchange and sending Bitcoins using such exchanges requires an "affirmative act" to execute the transaction, which is recorded on a public ledger.[2] As the first appellate court to weigh in on the issue, the Fifth Circuit's decision helps both Bitcoin users and law enforcement navigate this relatively new territory of virtual currencies and acts as a warning to users who seek anonymity by using Bitcoin for illicit transactions.[3]

II. BACKGROUND

A. Bitcoin, Blockchain, and Bitcoin Exchanges

Before seeing how courts analyze novel issues regarding Bitcoin, it is important to first have a general understanding of what Bitcoin is and how it is used. Although frequently discussed as a potentially worthwhile investment because of its volatility in price,[4] the technology behind how Bitcoin

---

* Daniel Penn is a 2022 Candidate for Juris Doctor at the SMU Dedman School of Law. He received a Bachelor of Science in Psychology from Texas Christian University.

1. United States v. Gratkowski, 964 F.3d 307, 312–13 (5th Cir. 2020).

2. *Id.* at 311–13.

3. *See id.* at 311–12.

4. *See* Ben Winck, *Bitcoin Rallies 4% to Surpass $14,000 as Election Volatility Fuels Cryptocurrency Surge*, BUS. INSIDER (Nov. 4, 2020, 1:36 PM), https://markets.businessinsider.com/currencies/news/bitcoin-price-hiits-14000-us-election-volatility-btc-cryptocurrency-market-2020-11-1029766585.

transactions take place is what brings Gratkowski's case to the Fifth Circuit.[5] According to its website, Bitcoin is "the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen."[6] Although lacking any "physical properties (like gold and silver)" or backing by a central government, Bitcoin instead derives its value through trust by people willing to accept Bitcoins in exchange for goods or services.[7]

The transparent-by-design nature of how Bitcoins function as a currency helps foster that trust because every transaction is permanently recorded on a public ledger known as the "blockchain."[8] Additionally, because anyone can access the Bitcoin source code and the blockchain cannot be modified, every aspect of how Bitcoin works can be verified and all transactions can be double-checked.[9] When a transaction occurs, each user's public Bitcoin address, as well as the amount of Bitcoin, is added to the blockchain to document the transfer.[10] A public Bitcoin address is a random string of twenty-six numbers and letters that designates either the sender or recipient of a transaction,[11] acting similarly to an email address without any indication as to who actually owns the account.[12] A private key, which should only be known by the Bitcoin address owner, is tied to each address and allows owners to spend the Bitcoins registered to that address by verifying the transaction.[13]

Many users opt to use third-party Bitcoin exchange websites to buy, sell, and transfer Bitcoin instead of downloading the necessary software to interact with the blockchain themselves.[14] Operating much like stock exchanges for buying ownership in publicly traded companies, these websites match those looking to buy with those willing to sell.[15] Coinbase, the exchange website discussed in the case, is a self-described "one stop shop" that also allows users to "store" their Bitcoins in virtual wallets through the web-

5. *See Gratkowski*, 964 F.3d at 309.

6. *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq#general (last visited June 9, 2021).

7. *Id.*

8. *Id.*

9. *Id.*

10. David Floyd, *How Bitcoin Works*, INVESTOPEDIA, https://www.investopedia.com/news/how-bitcoin-works/ (last updated June 30, 2020).

11. *Bitcoin Addresses Explained*, TOKENS24 (Nov. 14, 2017), https://www.tokens24.com/cryptopedia/basics/bitcoin-addresses-explained.

12. Floyd, *supra* note 10.

13. *Id.*

14. Jake Frankenfield, *Bitcoin Exchange*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bitcoin-exchange.asp (last updated July 13, 2020).

15. *Id.*

site in addition to serving as an exchange.[16] As part of creating an account, Coinbase requires users to verify their identity by uploading either a driver's license or state-issued ID card.[17] Once the user's identity is confirmed, they are free to buy, sell, and transfer Bitcoin with other users, including as payment on websites that accept it.[18]

B. Facts Leading to Gratkowski's Case

As part of an investigation into a child-pornography website in 2016, federal agents determined that users were paying for downloadable material from the website with Bitcoin.[19] Those agents, with the assistance of an outside service, then determined which Bitcoin addresses were linked to the website under investigation by analyzing the publicly-available Bitcoin blockchain.[20] To uncover more information about the website's users, agents then served a grand jury subpoena on Coinbase for information about any customers who had sent Bitcoin to the website's addresses.[21] Coinbase's response to the subpoena indicated that Gratkowski had transacted with the website, and the agents used this connection as probable cause to obtain a warrant to search his home.[22]

The execution of that search warrant led to Gratkowski's arrest after agents discovered a hard drive with almost 200 illicit images inside of his home.[23] During a subsequent interview with agents, Gratkowski admitted that he had visited the site in question, in addition to downloading files from multiple sites.[24] After being charged on a two-count indictment, Gratkowski quickly moved to suppress the evidence on the grounds that the government violated the Fourth Amendment by using a subpoena to obtain his information instead of a warrant.[25] However, the district court denied the motion.[26] Although the district court later vacated the initial denial *sua sponte*, it deter-

16. *What is Coinbase?*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/general-crypto-education/what-is-coinbase (last visited June 9, 2021).

17. *Identity Document Verification*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/verify-my-account/id-doc-verification (last visited June 9, 2021).

18. *How to Send and Receive Cryptocurrency*, COINBASE, https://help.coinbase.com/en/coinbase/trading-and-funding/cryptocurrency-trading-pairs/how-to-send-and-receive-cryptocurrency.html (last visited June 9, 2021).

19. United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020).

20. *Id.*

21. *Id.*

22. *Id.*

23. Brief of Appellee at 10, United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) (No. 19-50492).

24. *Id.*

25. *Id.*

mined that—even if Gratkowski had a reasonable expectation of privacy—the evidence was still admissible under the good-faith exception to the exclusionary rule.[27] Following the court's decision not to suppress the evidence, Gratkowski pled guilty to both counts, reserving the right to appeal the Fourth Amendment issue as part of his plea agreement.[28]

III. THE APPEAL

In hearing this appeal, the Fifth Circuit had to determine whether Bitcoin users have a Fourth Amendment privacy interest in either the information of their Bitcoin transactions stored on the Bitcoin blockchain or personal information provided to by the users Bitcoin exchanges like Coinbase.[29] In holding that there was no reasonable expectation of privacy, the court correctly reasoned that the public nature of the Bitcoin blockchain ledger combined with the voluntary disclosure of information to Bitcoin exchanges by the users negated the need for agents to obtain a warrant.[30] Specifically, the Fifth Circuit was not willing to adopt Gratkowski's argument that the Bitcoin blockchain and personal information collected by Coinbase deserved the same protection of cell phone location information,[31] which is protected by the Fourth Amendment.[32]

A. The Fifth Circuit Looks to Third-Party Doctrine Precedent for Guidance

Unpersuaded by Gratkowski's comparisons of Bitcoins to cell phone location records, the Fifth Circuit instead focused on why the Supreme Court considered location records worthy of protection, despite seeming to fit squarely within the third-party doctrine.[33] Typically, people forfeit any legitimate expectation of privacy in information "voluntarily turn[ed] over to third parties."[34] The Supreme Court in *United States v. Miller* applied this third-party doctrine to information contained in bank records because those records revealed information that customers had turned over to the banks voluntarily and were considered "negotiable instruments" rather than documents presumed to be confidential.[35]

26. *Id.* at 11.
27. *Id.*
28. *Id.*
29. *Gratkowski*, 964 F.3d at 310.
30. *See id.* at 311–12.
31. *Id.* at 312.
32. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
33. *Gratkowski*, 964 F.3d at 311.
34. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
35. United States v. Miller, 425 U.S. 435, 442 (1976).

Similarly, telephone call logs also fall within the third-party doctrine exception to the Fourth Amendment because placing a call requires the user to voluntarily convey the intended recipient by dialing the appropriate numbers, according to the Supreme Court in *Smith v. Maryland*.[36] But both *Miller*[37] and *Smith*[38] were decided decades before cell phones became popular and, thus, the Supreme Court had to determine if the technological advances in both the type of data collected and the manner in which it was acquired differed from call logs such that it was still obtainable without a warrant.[39] The Fifth Circuit, therefore, appropriately considered the rationale in *Carpenter* as guidance on whether the third-party doctrine was appropriate for information seemingly similar to bank records or if the nature of Bitcoin transactions is sufficiently distinguishable.[40]

In *Carpenter*, the Supreme Court weighed both the "nature of the particular documents sought" and the "voluntary exposure" in considering whether the government obtaining 127 days' worth of timestamped GPS data from a third-party phone company constituted a Fourth Amendment search, requiring a warrant.[41] Compared to phone call logs, the Court considered the nature of cell phone location information to be far more invasive because it "provides an intimate window into a person's life," while also being far easier, cheaper, and more efficient than "traditional investigative tools."[42] Additionally, the cell phone location information differs from phone calls because the user is not voluntarily offering their location to the provider by carrying a cell phone, but instead the information is more passively collected than actively dialing specific phone numbers.[43] As a result, the Supreme Court held that, even though the cell phone location information came from a third party, the intimate nature of the information and lack of an affirmative act by the user kept it under the protection of the Fourth Amendment; therefore, a warrant was necessary to obtain the information.[44]

B. The Court's Rationale for Not Extending Protection to Bitcoin Transactions

Weighing the same factors considered in *Carpenter*, the Fifth Circuit first considered whether Gratkowski had a reasonable expectation of privacy

36. *Smith*, 442 U.S. at 742.

37. *Miller*, 425 U.S. 435.

38. *Smith*, 442 U.S. 735.

39. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

40. *See* United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020).

41. *Carpenter*, 138 S. Ct. at 2219–20.

42. *Id.* at 2217–18.

43. *Id.* at 2220.

44. *Id.*

in his information on the Bitcoin blockchain.[45] As previously described, every Bitcoin transaction is permanently documented on the blockchain, which is accessible to anyone wanting to view it.[46] Specifically, the information stored on the public blockchain only consists of both parties' Bitcoin addresses and the amount of Bitcoin transferred.[47] The court considered the nature of this information to be limited and does not constitute "a pervasive [or] insistent part of daily life."[48] Additionally, the court noted that transferring Bitcoin "requires an affirmative act by the Bitcoin address holder."[49] Consequently, it determined that Gratkowski did not have a reasonable privacy interest in the information stored on the public Bitcoin blockchain.[50]

Turning next to Gratkowski's privacy interest in his Bitcoin transactions on Coinbase, the court again considers the nature of the information maintained in records by Coinbase and whether he voluntarily turned over that information.[51] Emphasizing that Coinbase is a financial institution and is regulated through the Bank Secrecy Act just like traditional banks, the court quickly concluded that the Coinbase records are more closely aligned with the bank records at issue in *Miller* than cell phone location information,[52] despite Gratkowski's efforts to convince them otherwise.[53] Without privacy interests in either his information on the blockchain or on Coinbase, the Fifth Circuit affirmed the trial court's denial of his motion to suppress and became the first appellate court to decide that Bitcoin transactions carried out through a third-party exchange are not entitled to Fourth Amendment protection.[54]

IV. ANALYSIS AND PRACTICAL IMPLICATIONS OF THE FIFTH CIRCUIT'S DECISION

In declining to extend Fourth Amendment protection to information stored on the blockchain and on exchange websites, the court correctly determined that, although the technology required for Bitcoin transactions is far more complicated than traditional currencies, third-party exchange websites are very similar to traditional banks from the user's perspective.[55] Both platforms provide users a place to keep their money, transfer it to other accounts,

45. *Gratkowski,* 964 F.3d at 311–12.

46. *Frequently Asked Questions*, *supra* note 6.

47. *Id.*

48. *Gratkowski*, 964 F.3d at 312.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. Brief of Appellee, *supra* note 23, at 17–18.

54. *Gratkowski*, 964 F.3d at 313.

55. *See generally id.* at 312–13.

and exchange it for other forms of currency.[56] As discussed by the court, these similarities are why Coinbase is a regulated financial institution through the Bank Secrecy Act and keeps records of its customers' identities.[57] Thus, the lure of Bitcoin as a potentially-anonymous form of payment is unobtainable when using an intermediary like Coinbase because, not only are Bitcoin transactions inherently transparent by design,[58] but they also cleanly fall within the third-party doctrine, allowing for the government to obtain customer information in bank records with a grand jury subpoena rather than a warrant.

A. Why Gratkowski's Fourth Amendment Argument Fails

In his appeal, Gratkowski attempted to argue that the analysis of the Bitcoin blockchain and subpoena served on Coinbase constituted searches requiring warrants and that the government's failure to obtain such warrants violated his Fourth Amendment right against unlawful search and seizure.[59] To support his argument, Gratkowski heavily relied on the Supreme Court's decision in *Carpenter* affording Fourth Amendment protection to cell phone location records,[60] in addition to the district court vacating the initial denial because the Coinbase records "may fall within the rule announced in *Carpenter*."[61]

Analogizing the Supreme Court's rationale in *Carpenter*, Gratkowski unsuccessfully argued that the Bitcoin blockchain's inherently public nature did not automatically preclude protection because "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[62] However, using Bitcoin as a form of payment goes well beyond merely "venturing into the public sphere."[63] By design, all Bitcoin transactions permanently become part of the blockchain in order to ensure transparency between parties and are viewable by any person that accesses the blockchain.[64] Although privacy concerns were clearly considered when determining what information would be recorded on the blockchain,[65] those concerns were addressed by only recording the Bitcoin addresses of both

56. *What Is Coinbase?*, *supra* note 16.

57. *Gratkowski*, 964 F.3d at 312.

58. *Frequently Asked Questions*, *supra* note 6.

59. Brief of Appellee, *supra* note 23, at 12.

60. Carpenter v. United States, 138 S. Ct. 2206, 2272 (2018).

61. Brief of Appellee, *supra* note 23, at 18–19.

62. *Id.* at 17.

63. *See id.*

64. *Frequently Asked Questions*, *supra* note 6.

65. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, https://bitcoin.org/bitcoin.pdf (last visited July 5, 2021).

parties and the amount.[66] On the surface, this would appear to support a finding that users have a reasonable expectation of privacy. Instead, however, the limited information publicly recorded almost completely solidifies the opposite conclusion because the lack of identifiable information heavily suggests that users would not have a privacy interest.[67]

Because the ledger does not directly contain identifying information,[68] Gratkowski notes that the government had to recruit a third party, who used "powerful and sophisticated software" to determine clusters of addresses related to the website.[69] That software, he argued, is similar to "the sense-enhancing technology in *Kyllo* that was 'not in general public use.'"[70] Although not addressed by the court in deciding this case, the Supreme Court held that the use of thermal imager to detect heat signatures from inside the defendant's home constituted a Fourth Amendment search because the government cannot capitalize on new sense-enhancing technology to gain the ability to see into a person's home without a warrant.[71]

This argument is not persuasive for two reasons. First, the thermal imager used in *Kyllo* allowed government agents to effectively "see" through walls that would otherwise completely prevent observation by detecting heat coming from individuals on the inside.[72] Without the thermal imager, government agents would not be able to see what was behind the homeowner's wall.[73] The Bitcoin blockchain, however, is publicly available for any user to analyze and verify.[74] The software used to detect address clusters does not give those using it the ability see previously-hidden information.[75] Instead, it simply allows the user to more efficiently analyze the publicly available blockchain.[76] Second, even if the court did consider the software to be sense-enhancing like the thermal imagers, the holding in *Kyllo* is only applicable when the government is exploring within the individual's home.[77] The Bitcoin blockchain, on the other hand, is not located within Gratkowski's

66. *Frequently Asked Questions*, *supra* note 6.

67. United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020).

68. *Frequently Asked Questions*, *supra* note 6.

69. Brief of Appellee, *supra* note 23, at 18.

70. *Id.*

71. Kyllo v. United States, 533 U.S. 27, 35 (2001).

72. *Id.*

73. *Id.*

74. *Frequently Asked Questions*, *supra* note 6.

75. Brief of Appellee, *supra* note 23, at 27–28.

76. *Id.*

77. *Id.* at 28–29.

home but rather on the peer-to-peer network that links computers from all around the world.[78]

B. Future Implications of the Fifth Circuit's Decision

Just as Bitcoin was the preferred payment method on the website[79] discussed in the *Gratkowski* case, Bitcoin has a long-standing reputation as an ideal currency for illicit transactions.[80] This reputation, in part, is likely due to its apparent ability to provide anonymity to users attempting to shield their identity by hiding behind their Bitcoin addresses.[81] The Fifth Circuit's decision, however, appears to cut against that apparent anonymity by declining to afford Fourth Amendment protection to Bitcoin wallets and information stored on the Bitcoin blockchain.[82] Could this decision, then, potentially help Bitcoin shake its connection with illegal activity and bolster confidence as a legitimate currency?

According to the *New York Times*, only one percent of all Bitcoin transactions actually involve illicit activity.[83] Although the amount of Bitcoin used for illegal activity is probably slightly higher due to people using legitimate means of purchasing Bitcoins in attempts to circumvent laws of their respective countries and, thus, making the percentage harder to accurately quantify,[84] the Fifth Circuit's decision in *Gratkowksi* could nevertheless help deter would-be criminals in the United States from using the virtual currency to carry out these illicit transactions.[85] Federal agents would no longer need to obtain a warrant—but instead just a grand jury subpoena—to uncloak their hidden identities due to the ID-verification requirement on sites such as Coinbase.[86] Combined with efforts to shut down dark net trading websites,[87] Bitcoin should soon be able to finally transition from its dark history with online crime to a new, established way to pay for services as more and more people begin to trust the currency, which is, after all, where Bitcoin's value itself is derived.[88]

78. *Frequently Asked Questions*, *supra* note 6.

79. United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020).

80. Nathaniel Popper, *Bitcoin Has Lost Steam. But Criminals Still Love It.*, N.Y. TIMES (Jan. 28, 2020), https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html.

81. *Id.*

82. *Gratkowski*, 964 F.3d at 310.

83. Popper, *supra* note 80.

84. *Id.*

85. *Identity Document Verification*, *supra* note 17.

86. *Id.*

87. Popper, *supra* note 80.

88. *Frequently Asked Questions*, *supra* note 6.

V. CONCLUSION

Being the first circuit decision regarding Bitcoin and the Fourth Amendment, there is always the possibility that another circuit might decide differently, or the Supreme Court could reverse the ruling. Although, given the logical analysis used by the Fifth Circuit and the inherently public nature of Bitcoin's blockchain, other circuits may instead opt to use this case as a guide should a similar issue arise. As a result, this decision should serve as a warning to individuals under the impression that using Bitcoin protects your identity when making illicit transactions. The lack of identifying information recorded on the blockchain might afford some privacy from the average person uncovering the parties involved in a transaction, but there is no reasonable expectation of privacy worthy of Fourth Amendment protection to that record or to the information stored by Coinbase.

The lack of Fourth Amendment protection could potentially serve as a deterrent for using Bitcoin and blockchain technology as a method of conducting illegal businesses, thus eliminating the negative stigma long-since associated with the technology.[89] Additionally, companies that were previously on the fence about the technology because of that stigma could be more receptive to adopting Bitcoin and blockchain into their business because the court has shown that it is helping to regulate the new technology by cracking down illicit uses. Therefore, the Fifth Circuit's decision could help propel Bitcoin's trajectory forward as an accepted currency by correctly deciding that Gratkowski was not entitled to Fourth Amendment protection when using Bitcoin for illicit activity.[90]

89. Popper, *supra* note 80.

90. United States v. Gratkowski, 964 F.3d 307, 310 (5th Cir. 2020).