NOTE

The Privacy Revolution Begins: Did *Carpenter* Just Give Bitcoin Users a Chance to Strike Down the Bank Secrecy Act?

*Christopher Lloyd**

ABSTRACT

The 21st century has seen tremendous advances in financial technology, many of which the American legal system is just beginning to understand. One technological development, the cryptocurrency known as "Bitcoin," holds the potential to both democratize access to capital and facilitate transactions without the need for a central actor. Unfortunately, Bitcoin can just as easily be used for nefarious activities such as money laundering, terrorist financing, and other financial crimes. As Bitcoin has become more mainstream, federal authorities have enjoyed some success applying existing laws—including the Bank Secrecy Act—to the Bitcoin ecosystem and cryptocurrency exchanges that facilitate the buying and selling of Bitcoin. Following the Supreme Court's recent and revolutionary decision in Carpenter v. United States*—which establishes a new framework for evaluating privacy in the digital age—however, the Bank Secrecy Act's constitutionality as applied to Bitcoin may be in jeopardy. This Note explores the impact* Carpenter *may have on the Bank Secrecy Act in the context of Bitcoin and what Congress can do to resolve that uncertainty. Because there is a significant possibility that* Carpenter*'s reasoning may be extended to protect certain data on the Bitcoin network, this Note urges Congress to amend the Bank Secrecy Act to lessen the chance that a constitutional challenge against the Act will be successful. In modifying the*

* J.D., expected 2020, The George Washington University Law School. I am grateful to Mark D. Taticchi and Patrick Hynds, whose feedback and mentorship were invaluable during the writing process.

Bank Secrecy Act, Congress can bolster privacy protections while simultaneously retaining law enforcement's ability to use the statute to combat the types of financial crimes the law was designed to stop.

Table of Contents

Introduction

For many Americans, June 22, 2018 was probably just another hot summer Friday. The New York Times's front page included stories

about changes in President Trump's Cabinet,[1] federal authorities' plans to house migrant children on military bases,[2] and the hidden messages behind First Lady Melania Trump's famous "I really don't care, do u" jacket.[3]

But later that day, in Washington, D.C., the Supreme Court made history by issuing a landmark decision—*Carpenter v. United States*[4]—that will likely have a tremendous impact on the daily lives of individual Americans for decades to come. Although the Court insisted its decision was a narrow one,[5] the case transformed Fourth Amendment jurisprudence by introducing a new framework for examining privacy protections in the digital age.[6] The Court took the first steps away from its traditional third-party doctrine—defining privacy rights in terms of whether a consumer voluntarily gives a third-party entity access to data—and held that several other factors, including "breadth[ ] and comprehensive reach"[7] of the data involved, should play a new role in crafting privacy protections. This novel framework, the full impacts of which are still unknown, is likely to affect future jurisprudence on Fourth Amendment protections as related to everything from cell phone data that details a user's every move[8] to wearable technologies that assemble increasingly detailed pictures of a user's personal health.[9] Today's data-rich technology is becoming more integrated into daily life,[10] and the legal system—led by the Supreme Court—is just beginning to determine how the Fourth Amendment should operate in this uncharted frontier.

One of these new technologies, Bitcoin, is rapidly changing the way average Americans access capital and, more broadly, how the financial payment industry operates.[11] Considered a "cryptocurrency,"

---

1 *See* Glenn Thrush & Erica L. Green, *Shaking Up Cabinet to Shrink the Government*, N.Y. TIMES, June 22, 2018, at A1.

2 *See* Michael D. Shear et al., *4 Military Bases Prepare to Hold 20,000 Children*, N.Y. TIMES, June 22, 2018, at A1.

3 *See* Vanessa Friedman, *First Lady's $39 Jacket Makes a Statement, but What Kind?*, N.Y. TIMES, June 22, 2018, at A1.

4 138 S. Ct. 2206 (2018).

5 *See id.* at 2220.

6 *See* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1374 (2019).

7 *Carpenter*, 138 S. Ct. at 2223.

8 *See id.* at 2216.

9 *See* James Swann, *Your Fitbit Steps May Not Be Protected by Federal Law,* BLOOMBERG L. (May 30, 2018, 9:00 AM), https://news.bloomberglaw.com/health-law-and-business/video-your-fitbit-steps-may-not-be-protected-by-federal-law [https://perma.cc/P532-TQG8].

10 *See* Olga Kharif, *The Internet of Things*, BLOOMBERG (Oct. 7, 2019, 4:45 AM), https://www.bloomberg.com/quicktake/internet-things [https://perma.cc/F8E3-8CHF].

11 *See* Rasmus Pihl, *International Monetary Fund Suggests Cryptocurrency Could Replace*

this supposedly decentralized payment and accounting system has seen its share of eternally optimistic promoters[12] and ever-cynical detractors.[13] Regulators are grappling with how to fit Bitcoin—with its lack of a central controlling entity[14]—into existing tax, securities, commodity, and money laundering rules and regulations.[15]

This Note will focus on the aftermath of *Carpenter* and the impact the decision may have on federal agencies' attempts to combat financial crimes within the Bitcoin network. The chief statutory vehicle empowering federal agents to investigate and combat these crimes—the Bank Secrecy Act ("BSA")[16]—accomplishes those goals via a comprehensive system of reporting, data collection, and anti–money laundering ("AML") rules that have long been applied to American banks and other qualifying financial institutions.[17] Before the Supreme Court even decided *Carpenter*, agencies such as the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") have been applying the BSA's provisions to certain cryptocurrency exchanges,[18] which facilitate the buying and selling of cryptocurrencies

---

Fiat Currencies, Toshi Times (June 7, 2018), https://toshitimes.com/international-monetary-fund-suggests-cryptocurrency-could-replace-fiat-currencies/ [https://perma.cc/6ECG-RSPX].

12 *See, e.g.*, Bloomberg Markets and Finance, *Novogratz Talks Cryptocurrencies and Regulation*, YouTube (June 5, 2018), https://www.youtube.com/watch?v=oWhzlaymNIk [https://perma.cc/TAS9-SZYE].

13 *See, e.g.*, Ali Montag, *Nobel-Winning Economist: Authorities Will Bring Down 'Hammer' on Bitcoin*, CNBC (July 9, 2018, 4:33 PM), https://www.cnbc.com/2018/07/09/nobel-prize-winning-economist-joseph-stiglitz-criticizes-bitcoin.html [https://perma.cc/KN3J-5696].

14 *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1, https://bitcoin.org/bitcoin.pdf [https://perma.cc/DC6C-HUWX].

15 *See* William Hinman, SEC Dir. Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018) (transcript available at https://www.sec.gov/news/speech/speech-hinman-061418 [https://perma.cc/VF5C-P2E2]); Kate Rooney, *SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies*, CNBC (June 6, 2018, 10:45 AM), https://www.cnbc.com/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html [https://perma.cc/8X2Y-NKX6].

16 Pub. L. No. 91-508, 84 Stat. 1118 (codified as amended in scattered sections of 12 & 15 U.S.C.).

17 *See* James Sivon, *Fintech and the Existing Legal Framework for Anti-Money Laundering and Counter-Terrorism Financing*, 18 No. 3 Fintech L. Rep. 8 (May/June 2015) ("The Bank Secrecy Act was passed in response to concerns over the use of secret foreign banking accounts to facilitate illegal activities and a lack of recordkeeping by banks to assist law enforcement agencies. The Act established recordkeeping and reporting requirements for financial institutions, including the submission of Currency Transaction Reports ('CTRs') to the federal government. It also established civil and criminal penalties for failure to comply with record keeping and reporting requirements. . . . [T]he legal framework established in the Bank Secrecy Act has evolved and been expanded over time, but the basic framework of the Act—recording and reporting financial transactions to federal authorities—has remained unchanged since 1970.").

18 *See* Press Release, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), https://www.FinCEN.gov/news/

such as Bitcoin in exchange for cash or even other cryptocurrencies.[19] The Court's opinion, which raises fresh questions about the Fourth Amendment's application to specific data sets and technologies—combined with Bitcoin's shared characteristics as both a digital asset and digital property—jeopardizes the BSA's application to entities within the Bitcoin space.

Because of this legal uncertainty, a criminal case in which law enforcement relies on the BSA for its enforcement authority will likely face the question of whether the BSA, under the Supreme Court's new guidelines, is constitutional as applied to transaction data on the Bitcoin network. A defendant facing charges for money laundering or other financial crimes may challenge the means federal authorities used to gather evidence of his alleged activities, especially if those authorities used a subpoena, instead of a warrant, to access those records.

To ensure that law enforcement's ability to operate in this new digital landscape is not unduly encumbered, Congress ought to make a minor linguistic but substantively significant change to the BSA's language. The BSA's broad framework—the recordkeeping and reporting regime to which qualifying financial institutions must adhere—should be left in place at least as that system relates to anonymous data points. Where law enforcement seeks to obtain more specific data to identify particular actors, Congress ought to statutorily require the use of a warrant and probable cause. Doing so will likely have minimal impact on law enforcement efficiency because the anonymous transaction data reported under the BSA will support probable cause. In that way, Congress will remove the cloud of constitutional uncertainty surrounding law enforcement investigations under the BSA while simultaneously protecting individual privacy in an increasingly digitized world and ensuring law enforcement can effectively protect the public.

This Note is organized as follows. Part I provides an overview of Bitcoin and federal authorities' current use of existing laws to regulate

---

news-releases/FinCEN-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual [https://perma.cc/E3LJ-SSRM].

19 *See* Press Release, U.S. Dep't of Justice, Acting Assistant Attorney General Mythili Raman Testifies Before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 18, 2013), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mythili-raman-testifies-senate-committee-homeland [https://perma.cc/6KEM-8B3D] ("A network of sites and services, including exchangers who buy and sell virtual currencies in exchange for national currencies or other mediums of value, have developed around virtual currency systems, as well.").

activity on the Bitcoin network. Part II details the history of federal efforts to combat money laundering through the BSA. Part II also explores how the Supreme Court, just a few years after the BSA's enactment, held that the law was constitutional under the Fourth Amendment. Part III provides an overview of the Supreme Court's Fourth Amendment jurisprudence with a special emphasis on the third-party doctrine: the primary rule that has long defined the contours of Americans' privacy rights. Part IV discusses *Carpenter* and the serious strains it places on existing Fourth Amendment jurisprudence and how *Carpenter* may make the BSA unconstitutional as applied to Bitcoin, despite the Supreme Court's insistence that the decision was narrow. Part V identifies how Congress, by requiring a warrant for personally identifying information, can amend the BSA to protect privacy rights while ensuring law enforcement has the necessary tools to effectively combat financial crimes on the Bitcoin network.

I. Bitcoin: Property or Digital Record?

A. History of Bitcoin

Bitcoin was once just another novel and obscure computer technology only the most dedicated coding aficionados studied. A mysterious computer programmer operating under the name "Satoshi Nakamoto" first proposed this digitally-based currency and payment system as "an electronic payment system based on cryptographic proof instead of trust."[20] The idea was simple: allow any two willing parties to transact with each other without the need for a trusted third party via a secure network incapable of being manipulated by nefarious actors.[21] For many years, Bitcoin was little more than a thought-provoking experiment, with per-coin values averaging a mere eight cents.[22] Nine years later, however, mania ensued, and Bitcoin reached an all-time high of almost $20,000 as financial speculators and retail investors alike flocked to participate in this new investment option.[23] Several large financial institutions, including Goldman Sachs, announced intentions to create trading desks devoted entirely to

---

20 Nakamoto, *supra* note 14, at 1.

21 *See id.*

22 *See* Tracy Alloway, *After the Crazy, the Reality*, Bloomberg Businessweek, Dec. 17, 2018, at 44.

23 *See* Sam Ouimet, *Down More than 70% in 2018, Bitcoin Closes Its Worst Year on Record*, Coindesk (Jan. 2, 2019, 3:32 PM), https://www.coindesk.com/down-more-than-70-in-2018-bitcoin-closes-its-worst-year-on-record [https://perma.cc/YC8B-V6YT].

cryptocurrencies such as Bitcoin.[24] Unfortunately for latecomers, Bitcoin soon experienced a subsequent collapse far more precipitous than its incredible rise. One year after that all-time, intraday high, Bitcoin was worth just above $4,000 per coin,[25] and rumors swirled that institutional banks were abandoning the crypto space.[26]

At the time of this Note's writing, individual Bitcoins are worth just above $8,000.[27] Even as financial analysts debate the value of each coin and economists consider this cryptocurrency's long-term impacts on the global financial industry, Bitcoin continues to capture the interests of investors, speculators, law professors,[28] and—perhaps most importantly—regulators.

Public perception of Bitcoin is sharply divided. On one side are the currency's most avid proponents, who argue that despite Bitcoin's recent collapse in value, the currency will one day replace fiat currencies and usher in an era of decentralized finance.[29] These supporters argue that Bitcoin embodies the type of trust and confidence centralized banks are incapable of providing anymore.[30] Meanwhile, Bitcoin's detractors, including legendary investors such as Warren Buffet[31] and Steve Eisman,[32] insist the "currency" is a risky and speculative investment more appropriate for gamblers, speculators, and money launderers. This latter group includes those who argue Bitcoin's days as an unregulated financial product are limited.[33] It also

---

24 *See* Paul Vigna et al., *Goldman Sachs Explores a New World: Trading Bitcoin*, WALL STREET J. (Oct. 2, 2017, 8:00 PM), https://www.wsj.com/articles/goldman-sachs-explores-a-new-world-trading-bitcoin-1506959128 [https://perma.cc/W7SY-GT2N].

25 *See* Alloway, *supra* note 22.

26 *See* Kate Rooney, *Goldman Sachs CFO Says Bank Is Working on Bitcoin Derivative for Clients*, CNBC (Sept. 6, 2018, 7:21 PM), https://www.cnbc.com/2018/09/06/goldman-sachs-cfo-calls-reports-of-shutting-down-crypto-desk-fake-news.html [https://perma.cc/9YAG-HR8C].

27 *See* Bitcoin (USD) Price as of Jan. 11, 2020, COINDESK, https://www.coindesk.com/price/ [https://perma.cc/3PPU-HS4R] (adjust date range in top-right corner of graph).

28 *See* Eleanor Lumsden, *The Future Is Mobile: Financial Inclusion and Technological Innovation in the Emerging World*, 23 STAN. J.L. BUS. & FIN. 1, 42–43 (2018).

29 *See, e.g.*, Pihl, *supra* note 11.

30 *See* Lawrence Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 1, 21 (2014) (citing James J. Angel & Douglas McCabe, *The Ethics of Payments: Paper, Plastic, or Bitcoin?*, 132 J. BUS. ETHICS 603, 605–10 (2015)).

31 *See* Daniel Roberts, *Warren Buffet on Buying Bitcoin: 'That Is Not Investing,'* YAHOO FIN. (Apr. 28, 2018), https://finance.yahoo.com/news/warren-buffett-buying-bitcoin-not-investing-110702015.html [https://perma.cc/2SYP-UVL3].

32 *See 'Big Short' Investor Steve Eisman on Bitcoin and Crypto*, CNBC (May 17, 2018, 7:51 AM), https://www.cnbc.com/video/2018/05/17/big-short-investor-steve-eisman-on-bitcoin-and-crypto.html?play=1 [https://perma.cc/58VR-68UQ].

33 *See* Angela Monaghan, *Bitcoin Is a Fraud That Will Blow Up, Says JP Morgan Boss*,

includes those who believe regulators' recent focus on Bitcoin as a way to protect their own turf presents too many risks for the average investor.[34] What is undeniable, however, is that Bitcoin, cryptocurrencies, and their underlying technology are all here to stay and still hold tremendous potential to revolutionize industries from finance[35] to healthcare.[36]

B. How Bitcoin Works

Simply described, Bitcoin and similar cryptocurrencies are designed to function as an alternative to traditional financial payment processing systems. Outside of cryptocurrencies, payments between two parties usually depend on a centralized, third-party intermediary, such as a bank or credit card company, who serves as a gatekeeper that identifies the parties and guarantees the availability of funds.[37] In contrast, cryptocurrencies such as Bitcoin leverage technology to allow two parties to transact directly with each other, creating "peer to peer transaction networks."[38] In theory, Bitcoin's decentralized network, use of encrypted keys, and redundant ledger system will prevent any one individual, group of programmers, or central entity from destroying or manipulating Bitcoin's underlying value.[39]

To eliminate intermediaries, Bitcoin operates on technology called the "blockchain," a distributed ledger system that utilizes a network of servers and computers to maintain records without any one master or original copy.[40] Each computer or server is known as a "node," and is responsible for storing a local copy of the network's

---

GUARDIAN (Sept. 13, 2017, 6:26 AM), https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers [https://perma.cc/D259-BTT2].

34 *See* Montag, *supra* note 13; Kenneth Rogoff, *Bitcoin's Price Bubble Will Burst Under Government Pressure*, GUARDIAN (Oct. 9, 2017, 8:00 AM), https://www.theguardian.com/technology/news-blog/2017/oct/09/bitcoin-price-bubble-government-cryptocurrency [https://perma.cc/668Y-8HMG].

35 *See* Jonathan Rohr & Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, 70 HASTINGS L.J. 463, 464–65 (2019).

36 *See* Randy Bean, *Will Blockchain Transform Healthcare?*, FORBES (Aug. 5, 2018, 8:19 PM), https://www.forbes.com/sites/ciocentral/2018/08/05/will-blockchain-transform-healthcare/#48c5c1ca553d [https://perma.cc/L9Y6-2YAN].

37 *See* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 148–49 (2016).

38 *See* U.S. Dep't of Justice, *supra* note 19 ("Decentralized systems such as Bitcoin, which have no centralized administrating authority and instead operate as peer-to-peer transaction networks, entered the scene relatively recently but are growing rapidly.").

39 *See* Nakamoto, *supra* note 14, at 3–4.

40 *Id.*

transaction data.[41] There is no central "node" or server farm through which transactions must past for verification.[42] Users store their Bitcoins in accounts known as "wallets," which one commentator says "are really just computer memory storage units."[43] Bitcoin's underlying algorithm controls the movement of coins and records transaction history as users send or receive payments.[44]

Critical to this Note are the "keys" involved in sending and receiving Bitcoins. As mentioned earlier, Bitcoin users use accounts known as "wallets" to store their coins and transact with other users. There are no limits on the number of wallets an individual can own, and a single user can theoretically have hundreds or even thousands of wallets.[45] Each wallet, however, has two network-generated keys that are critical for access:[46] (1) a public key that serves as an address all other users can see and to which they can send Bitcoins, and (2) a private key that serves as a password required to "unlock" the wallet. The public key, which appears to other users as nothing more than a string of number and letters,[47] is recorded on network ledgers each time that wallet is involved in a transaction. The private key, meanwhile, is only accessible to the wallet's owner and is encrypted for another level of protection. An account cannot be used to send money without the private key, and other users cannot access funds received without their own private key. Because neither the public nor private keys include any personally identifying information, Bitcoin offers at least a theoretical level of anonymity.[48]

After a user completes a transaction on the Bitcoin network, the data associated with that transaction—date and time, public keys involved, and amounts transferred—is immediately, irreversibly, and

---

41 Jesse Marks, *Distributed Ledger Technologies and Corruption: The Killer App?*, 20 COLUM. SCI. & TECH. L. REV. 42, 44 (2018).

42 *Id.*

43 Nicholas Godlove, *Regulatory Overview of Virtual Currency*, 10 OKLA. J.L. & TECH. 1, 18 (2014).

44 *See* Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 501 (2018).

45 *See* Michael Scott, *Doing the Dance: The Art of Managing Multiple Bitcoin Wallets*, BTCMANAGER (Jan. 11, 2017), https://btcmanager.com/the-art-of-managing-multiple-bitcoin-wallets/?q=/the-art-of-managing-multiple-bitcoin-wallets/& [https://perma.cc/9D7J-G6LE].

46 *See* Evangeline Ducas & Alex Wilner, *The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada*, 72 INT'L J. 538, 545, 556 (2017).

47 *See* Werbach, *supra* note 44.

48 *See* Harsh Agrawal, *Bitcoin Private Keys: Everything You Need to Know*, COINSUTRA (Nov. 19, 2019), https://coinsutra.com/bitcoin-private-key/ [https://perma.cc/HCG4-WATW].

publicly cataloged on each ledger connected to the Bitcoin network.[49] The duplication of transaction history and lack of a single, central access point through which all transactions must flow and be recorded, which is typical of traditional payment processing systems, in theory lowers the chance of theft, fraud, or transaction history manipulation.[50] To commit an act of fraud or currency manipulation, a nefarious actor would need to alter the ledgers of every single node connected to the ecosystem before any one of those nodes recognized the discrepancy.[51]

Together, these technological innovations are intended to enable the Bitcoin ecosystem to operate independent of centralized systems[52] and provide easier access to capital at a time when faith in fiat currencies and central banks has plummeted.[53] The hope is that collective and anonymous cooperation among hundreds if not thousands of independent operators can provide a new and unassailable level of security and stability.[54]

C. Bitcoin's Success Sparks Government Interest

The rapid success of Bitcoin and other cryptocurrencies has caught the interest of government regulators around the world, with some countries going as far as banning the technology entirely.[55] In the United States, state and federal agencies are generally friendlier to Bitcoin, even if regulatory strategies among particular agencies differ. Financial regulators, for example, have struggled with determining reasonable accommodations to Bitcoin while providing investors with the same protections that other financial products' rules provide.

---

49 *See* Adem Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, arXiv .org (Mar. 29, 2018), https://arxiv.org/pdf/1801.03998.pdf [https://perma.cc/TPD6-R52X].

50 *See* Nakamoto, *supra* note 14, at 3; *Frequently Asked Questions: What Is Bitcoin?*, Bitcoin, https://bitcoin.org/en/faq#what-is-bitcoin [https://perma.cc/Q8LZ-D9SL].

51 *See* Elizabeth Sara Ross, Note, *Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues*, 25 Cath. U. J.L. & Tech. 353, 360–61 (2017).

52 *See* Trautman, *supra* note 30.

53 *See* John Cassidy, *The Real Cost of the 2008 Financial Crisis*, New Yorker (Sept. 10, 2018), https://www.newyorker.com/magazine/2018/09/17/the-real-cost-of-the-2008-financial-crisis [https://perma.cc/3G6Q-A29D].

54 *See* Maria Konash, *Blockchain: A Step Towards Decentralization or Another Form of Centralization*, Coinspeaker (Sept. 11, 2018, 1:26 PM), https://www.coinspeaker.com/blockchain-a-step-towards-decentralization-or-another-form-of-centralization [https://perma.cc/3G6Q-A29D]; *Everything You Need to Know About Bitcoin Mining*, bitcoinmining.com, https://www.bitcoinmining.com [https://perma.cc/2LGT-8LVE].

55 *See* Melanie L. Fein, *Bitcoin: How Is It Regulated?* 61 (Feb. 1, 2018) (unpublished manuscript) (available at https://ssrn.com/abstract=3166894 [https://perma.cc/2LGT-8LVE]).

The Internal Revenue Service, sensing the need to extend its rules to Bitcoin transactions and holdings, treats the cryptocurrency as property for tax purposes.[56] At the same time, the Commodity Futures Trading Commission—noticing the growth in Bitcoin future and derivatives trading markets—now classifies the asset as a commodity.[57] Meanwhile, the Securities and Exchange Commission, the federal government's primary securities exchange regulator, has taken a largely bifurcated approach. Initial coin offerings, through which cryptocurrency regulators offer a "token" or "coin" on their network in exchange for capital funding, are considered securities and subject to all the rules and regulations under the Securities Act of 1933[58] and the Securities Exchange Act of 1934.[59] By contrast, cryptocurrencies that have already scaled and are decentralized because they are not dependent on a single entity—including Bitcoin and another cryptocurrency known as "Euretheum"—are not considered securities by the agency.[60] The uncertainty these inconsistent regulatory frameworks produce is a serious problem for start-up cryptocurrency companies as well as established financial entities trying to join the cryptocurrency mania.

D. Current Enforcement Efforts

Separate to the regimes mentioned above—and most important to this Note—are actions taken by federal law enforcement agencies in fighting crime on the Bitcoin ecosystem. Relying on its authority under the federal government's primary AML statute—the BSA—entities such as the Treasury Department's FinCEN are using existing statutes and regulations to combat Bitcoin-enabled criminal activity.[61] In 2015, for example, FinCEN took its first civil action against a cryptocurrency exchange for failing to register as a money service business ("MSB") under the BSA.[62] In 2017, the agency took its second

---

56 *See id.* at 35.

57 *See id.* at 29.

58 Pub. L. No. 73-22, 48 Stat. 74 (1933) (codified at 15 U.S.C. §§ 77a–77bbbb).

59 Pub. L. No. 73-291, 48 Stat. 881 (1934) (codified at 15 U.S.C. §§ 78a–78qq); *see* Fein, *supra* note 55, at 16.

60 *See* Hinman, *supra* note 15; Rooney, *SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies*, *supra* note 15; *Spotlight on Initial Coin Offerings (ICOs)*, SEC (Apr. 11, 2019), https://www.sec.gov/ICO [https://perma.cc/ZK2K-N349].

61 For an overview of FinCEN's early work in applying the Bank Secrecy Act to the Bitcoin network, see generally Trautman, *supra* note 30.

62 *See In re* Ripple Labs Inc., Treas. Order 2015-05 (May 5, 2015) (assessment of civil money penalty).

action against a separate exchange for the same violation.[63] FinCEN's success in both of these cases is extremely important because these companies, once registered with FinCEN, have ongoing reporting and monitoring responsibilities under the BSA. MSBs must, among other things, "implement an effective anti-money laundering (AML) program . . . detect suspicious transactions and file suspicious activity reports (SARs), and . . . obtain and retain records relating to transmittals of funds in amounts of $3,000 or more."[64]

Unfortunately, FinCEN's continued ability to use this statute—a law that forms the core of the federal government's AML efforts—to gather information on Bitcoin crime may be at risk. The Supreme Court's decision in *Carpenter* leaves open the possibility that the BSA's regime—as applied to Bitcoin—may be struck down as unconstitutional.

II. The Bank Secrecy Act

A. *Overview*

Congress passed the BSA in 1970 to give the federal government new tools in the fight against financial crime.[65] Recognizing that these types of crimes are often difficult to detect, the statute created a reporting and recordkeeping regime utilized by the federal government but maintained by qualifying financial institutions.[66] As one commentator has stated, the BSA's "requirements effectively mandate the creation of a paper trail for large currency transactions, giving law enforcement authorities a way to 'follow the money' and detect criminal activity."[67] Qualifying institutions,[68] including banks and MSBs as

63 *See In re* BTC-E, Treas. Order 2017-03 (July 26, 2017) (assessment of civil money penalty).

64 *Id.* at 3.

65 *See* H.R. Rep. No. 91-975, at 10 (1970) ("According to law enforcement officials, an effective fight on crime depends in large measure on the maintenance of adequate and appropriate records by financial institutions. H.R. 15073 deals with the problem by requiring the maintenance of records by financial institutions in a manner designed to facilitate criminal, tax and regulatory investigations and proceedings.").

66 31 U.S.C. § 5311 (2012) (the Bank Secrecy Act "require[s] certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities . . . ."); *see* Courtney J. Linn, *Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring*, 50 Santa Clara L. Rev. 407, 428 (2010) (explaining Congress' reasoning for enacting the BSA's framework); Jonathan J. Rusch, *Hue and Cry in the Counting-House: Some Observations on the Bank Secrecy Act*, 37 Cath. U. L. Rev. 465, 467–68 (1988) (describing the four main types of reports certain financial institutions and other persons must file under the Bank Secrecy Act).

67 Linn, *supra* note 66, at 429.

well as certain non–financial institutions, are required to both record and report certain financial data, transactions,[69] and the personally identifying information[70] associated with those transactions and accounts to the appropriate federal law enforcement agency.[71] The BSA targets three categories of transactions: those involving amounts above $10,000,[72] those involving foreign bank accounts owned by American citizens with account balances greater than $10,000,[73] and other activities bank employees deem suspicious.[74] If a bank identifies activity falling into any one of these categories, it must submit an SAR to the appropriate federal authority.[75] The idea is to create a comprehensive database that investigators can later use to prosecute complex and otherwise hidden financial schemes.[76] Ultimately, the BSA's reporting requirements are intended to "drive money launderers, terrorists, and other criminals to evade [the requirements] and, in doing

68 *See* 31 U.S.C. § 5312(a)(2) (2012).

69 *See id.* §§ 5313–5316.

70 *See id.* § 5318(a)(2) (authorizing the Treasury Secretary to require covered financial institutions establish procedures to meet their obligations under the Bank Secrecy Act); U.S. DEP'T OF TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-2018-G001, GUIDANCE: FREQUENTLY ASKED QUESTIONS REGARDING CUSTOMER DUE DILIGENCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS (2018), https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf [https://perma.cc/Y6UG-UEVH] (describing how the Bank Secrecy Act requires identification of an account's beneficial owner(s) including the owner's "name, date of birth, address, and identifying number (such as a social security number or other identifying number . . .)").

71 12 C.F.R. § 208.62 (2019); *see* Douglas King, Banking Bitcoin-Related Businesses 6 (Feb. 2016) (unpublished working paper), https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/2016/banking-bitcoin-related-businesses.pdf [https://perma.cc/A9EW-KAYN].

72 *See* 31 U.S.C. § 5316(a); 31 C.F.R. § 103.22(b) (2010) (requiring the reporting of accounts that see greater than $10,000 in cash transactions in one day).

73 *See* 31 U.S.C. § 5314; 31 C.F.R. § 103.33(c) (2003) (requiring financial institutions to keep records of transactions to foreign accounts if the transaction exceeds $10,000); 31 C.F.R. § 103.24 (1998) (requiring reporting of foreign financial accounts to the Commissioner of the Internal Revenue Service).

74 *See* 31 C.F.R. § 1020.320(a)–(b) (2011) (requiring filing of certain transactions with FinCEN where activity indicates an intent to evade Bank Secrecy Act reporting rules); *see also* Matthew R. Hall, Note, *An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report*, 84 KY. L.J. 643, 653 (1996) (noting that the Bank Secrecy Act authorizes the Secretary of the Treasury to issue regulations requiring banks to report suspicious activity).

75 *See* 12 C.F.R. § 21.11 (2012) (requiring banks to file SARs on suspicious or obvious violations of AML laws or Bank Secrecy Act provisions); *id.* § 163.180(d) (requiring savings and service corporations to file SARs on suspicious or obvious violations of AML laws or Bank Secrecy Act provisions).

76 *See* H.R. REP. NO. 91-975, at 10 (1970).

so, to engage in evasive behavior that increases their risk of detection and prosecution."[77]

The bar for law enforcement to access these records is low.[78] Once law enforcement—through its own monitoring of the BSA's reports—becomes aware of suspicious activity, it need only obtain a subpoena to access an individual user's financial history.[79] In certain circumstances when a subpoena may not be feasible, law enforcement can access the data with as little as a formal written request.[80] Nowhere in the BSA is a warrant required or even encouraged.

B. United States v. Miller *Challenge*

The BSA's provision for a warrantless search of a customer's financial history has already seen at least one constitutional challenge, raised just six years after the BSA's enactment.[81] In *United States v. Miller*,[82] a defendant charged with unlawfully operating a distillery challenged his conviction for tax fraud, arguing that the government obtained some of its evidence against him in violation of his Fourth Amendment privacy rights.[83] The government used what the court of appeals called "a defective subpoena"[84] to obtain the defendant's "checks, deposit slips, two financial statements, and three monthly statements" for accounts he held at local banks.[85] The defendant contended that the government's failure to use a warrant constituted an unconstitutional search and seizure.[86]

---

77 Linn, *supra* note 66, at 434.

78 *See* 12 U.S.C. §§ 3405, 3408 (2012).

79 *See id.* § 3405 ("A Government authority may obtain financial records under section 3402(2) of this title pursuant to an administrative subpena [sic] or summons otherwise authorized by law . . . ."); *id.* § 3407 ("A Government authority may obtain financial records under section 3402(4) of this title pursuant to judicial subpena [sic] . . . .").

80 *See id.* § 3408 ("A Government authority may request financial records under section 3402(5) of this title pursuant to a formal written request . . . .").

81 *See* United States v. Miller, 425 U.S. 435, 442 (1976) ("Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy.").

82 *Id.*

83 *See id.* at 441 ("But respondent contends that the combination of the recordkeeping requirements of the Act and the issuance of a subpoena to obtain those records permits the Government to circumvent the requirements of the Fourth Amendment by allowing it to obtain a depositor's private records without complying with the legal requirements that would be applicable had it proceeded against him directly.").

84 *Id.* at 437.

85 *Id.* at 438.

86 *See id.* at 438–39.

A 7–2 Court disagreed, holding instead that the defendant had "no legitimate 'expectation of privacy'" in the records obtained.[87] The Court reasoned that the defendant could not possibly have believed his information would remain private because it "contain[ed] only information [he] voluntarily conveyed to the banks."[88] This standard quickly became known as the "third-party doctrine" test for whether records—especially business records—were protected by the Fourth Amendment.[89] For the Court, the defendant's lack of a Fourth Amendment privacy interest meant the government did not need to obtain a warrant.[90]

C. Subsequent Legislation

Wanting to preserve some sense of privacy post-*Miller*, Congress passed The Right to Financial Privacy Act in 1978.[91] This legislation bolstered Americans' privacy rights in financial records by requiring the government to notify a customer when it was about to access those records and afforded customers "an opportunity to challenge the government's actions in court."[92] Because Congress kept the BSA's subpoena process intact, in practice, The Right to Financial Privacy Act only marginally increased Americans' privacy interests.[93] Unfortunately, even those small increases in privacy have not survived. The 2001 Patriot Act[94]—designed to combat terrorist financing networks—severely eroded what little privacy Congress had given Americans in 1978.[95] Entities required to report data under the Patriot Act were permitted to transmit that data without notifying the customer.[96] And when the government sought the data for national security reasons, the Patriot Act effectively foreclosed "the possibility of judicial intervention."[97]

Today, the core of the BSA is still intact. It remains the central legislation upon which AML and "combating the financing of terror-

87 *Id.* at 442.

88 *Id.*

89 *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006).

90 *See Miller*, 425 U.S. at 446.

91 Pub L. No. 95-630, 92 Stat. 3641, 3697; *see* 1 WILLIAM E. RINGEL, SEARCHES & SEIZURES, ARRESTS AND CONFESSIONS § 8.31 (2d ed. 2003).

92 RINGEL, *supra* note 91, § 8.31.

93 *See* Robert J. Olejar, *Anti-Money Laundering v. the Right to Privacy*, N.J. LAW. MAG., Apr. 2008, at 56, 60–61.

94 Pub. L. No. 107-56, 115 Stat. 272.

95 *See* Olejar, *supra* note 93, at 56, 60–61.

96 *See id.* at 60.

97 *Id.*

ism"[98] reporting regimes are based. The BSA's subpoena process is still in place,[99] which offers little to no financial privacy.[100]

D. Bank Secrecy Act & Bitcoin

Since its enactment, the BSA's reporting requirements have been regularly and routinely applied to banks and other qualifying financial institutions.[101] One of the BSA's core reporting requirements covers entities known as MSBs and facilitates "the acceptance of currency, funds, or other value that substitutes for currency from one person . . . to another location or person by any means."[102] Well-known companies such as PayPal[103] and Western Union[104] fall under the BSA's registration and reporting requirements, as do foreign entities meeting the statutory definition above.[105]

In 2013, recognizing the proliferation of virtual currencies and virtual currency exchanges, FinCEN issued guidance asserting its authority to regulate those exchanges as MSBs.[106] FinCEN has since succeeded in extending the BSA's recordkeeping requirements to qualifying cryptocurrency entities. FinCEN, thus far, has focused its efforts on qualifying entities that failed to register as MSBs under the BSA.[107] And despite legal challenges to those enforcement actions, federal courts have concluded in at least six lawsuits that FinCEN does have the authority to include exchanges under the BSA.[108] En-

---

98 *See* Olejar, *supra* note 93, at 60.

99 *See* 12 U.S.C. § 3402 (2012); RINGEL, *supra* note 91, § 8.31.

100 *See* Olejar, *supra* note 93, at 60.

101 *See* 31 C.F.R. §§ 1010–60 (2018) (outlining the Department of Treasury's promulgation of regulations under the Bank Secrecy Act covering banks, casinos, MSBs, securities brokers and dealers, mutual funds, and other financial entities, all in an effort to broaden FinCEN's scope and combat financial crimes).

102 31 C.F.R. § 1010.100(ff)(5)(i)(A); *see also id.* § 1022 (detailing reports that MSBs must make to federal authorities and reports that MSBs must retain internally).

103 *See* FINCEN, *MSB Registrant Search*, https://www.FinCEN.gov/msb-registrant-search [https://perma.cc/BW5P-EKC2] (insert "Paypal" into the "Legal Name" search field).

104 *See id.* (insert "Western Union" into the "Legal Name" search field).

105 *See* Bank Secrecy Act Regulations, 76 Fed. Reg. 43585, 43589 (proposed July 21, 2011) (to be codified at 31 C.F.R. §§ 1010–1022).

106 *See* U.S. DEP'T OF TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [https://perma.cc/9W56-KQSC] ("This guidance refers to the participants in generic virtual currency arrangements, using the terms 'user,' 'exchanger,' and 'administrator.'").

107 *See In re* Ripple Labs Inc., Treas. Order 2015-05 (May 5, 2015) (assessment of civil money penalty).

108 *See* United States v. Mansy, No. 2:15-cr-198-GZS, 2017 WL 9672554, at *1 (D. Me. May 11, 2017) (citing United States v. Murgio, 209 F. Supp. 3d 698, 707 (S.D.N.Y. 2016)); United

forcement against cryptocurrency money laundering schemes may be in its early stages,[109] but FinCEN appears to enjoy the backing of federal courts. Consequently, FinCEN is likely to ramp up its efforts to expand the scope of the BSA and, by extension, gain more access to transaction data involving Bitcoin and other cryptocurrencies.

III. The Fourth Amendment Evolves

The Fourth Amendment contains language familiar to legal scholars, students of constitutional law, and lay citizens:

> 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.[110]

From the time of ratification until the mid-20th century, the Supreme Court's Fourth Amendment jurisprudence analyzed Americans' privacy rights through a property rights lens.[111] But that all changed when the Supreme Court announced its 1967 decision, *Katz v. United States*.[112] The Supreme Court's new test did not ask whether property was involved but instead whether Americans had a "reasonable expectation of privacy."[113]

Nine years later, the Court faced the particular question of whether Americans had a reasonable expectation of privacy in their

---

States v. Faiella, 39 F. Supp. 3d 544, 545–46 (S.D.N.Y. 2014); *see also* United States v. Budovsky, No. 13-cr-368, 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (listing 18 U.S.C. § 1960 as encompassing businesses that transmit virtual currency); United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 88–93 (D.D.C. 2008) (same); *cf.* United States v. Ulbricht, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014) (determining that bitcoins fall within the purview of the money laundering statute, 18 U.S.C. § 1956).

109 *See* Yogita Khatri, *New York State Sees First Conviction for Crypto Money Laundering*, Coindesk (Apr. 24, 2019, 12:00 PM), https://www.coindesk.com/new-york-state-sees-first-conviction-for-crypto-money-laundering [https://perma.cc/PMC2-6N5X].

110 U.S. Const. amend. IV.

111 *See* United States v. Jones, 565 U.S. 400, 405–06 (2012).

112 389 U.S. 347 (1967); *see* Gregory M. Caskey, California Search and Seizure § 2.5 (2019) (ebook) ("The Court un-tethered the [F]ourth [A]mendment's protection of privacy, security and liberty from common-law trespass in *Katz v. U.S.*"); Nicholas A. Kahn-Fogel, Katz*,* Carpenter*, and Classical Conservatism*, Cornell J.L & Pub. Pol'y (forthcoming 2019) (manuscript at 6) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3279871 [https://perma.cc/F9SP-6TX4]) ("Thus, in *Katz* the Court declared the property-based rubric for identifying Fourth Amendment searches to be 'discredited.'" (quoting *Katz*, 389 U.S. at 353)).

113 *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

bank and other financial records.[114] Deciding to take yet another turn in Fourth Amendment jurisprudence in *Miller*, the Court held that an individual's sharing of otherwise private information meant the user assumed the risk that the information would become public, thereby abrogating any privacy right in that information.[115]

Just three years later, the Supreme Court decided to extend *Miller*'s third-party doctrine to other types of business records, specifically records created when using a telephone company's services.[116] In *Smith v. Maryland*, Baltimore police decided to place the suspect in a robbery case under more surveillance.[117] Following a non-warrant police request, the telephone company that serviced the defendant's home added a pen register device to his line.[118] The device did not record the content of conversations but instead recorded "the numbers dialed from the telephone at petitioner's home."[119] The suspect challenged the police's warrantless collection of that data as a violation of his Fourth Amendment rights.[120] The Supreme Court rejected his argument, holding that, like the defendant in *Miller*, the suspect had no privacy interest in these business records.[121] Without a privacy interest, Baltimore police could obtain the records without a warrant.[122]

This landscape—where sharing information with third parties essentially destroys one's ability to claim privacy rights—stood firm for more than 40 years. With the advent of new technologies, specifically Global Positioning System ("GPS") technology, the Court soon faced new challenges to its longstanding jurisprudence.

The first cracks in the third-party doctrine occurred in the 2014 case of *Riley v. California*,[123] in which the Court flatly rejected the government's contention that, as the University of Pennsylvania's David Harris characterizes it, "officers seizing a phone should always have the authority to search the phone's call log without having to

114 *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

115 *See id.*

116 *See* 442 U.S. 735, 736 (1979).

117 *See id.* at 737.

118 *See id.*

119 *Id.*

120 *See id.*

121 *See id.* at 745.

122 *See id.* at 745–46.

123 134 S. Ct. 2473 (2014).

obtain a warrant."[124] The Supreme Court, recognizing the changing nature of technology in the digital age, noted that smartphones "hold for many Americans 'the privacies of life.'"[125] Nevertheless, the Court seemed to keep *Smith*'s application of the third-party doctrine to telecommunications alive.[126]

The first major challenge occurred in *United States v. Jones*,[127] in which prosecutors successfully convicted the owner of a District of Columbia nightclub for narcotics distribution following law enforcement's warrantless tracking of his movements via a GPS system.[128] The owner challenged the collection of those records under the Fourth Amendment.[129] Finding that he had a reasonable expectation of privacy in his movements, the Supreme Court upheld the D.C. District Court's reversal of the conviction.[130]

Although the Court's reasoning was certainly important, the most relevant portions of *Jones* for purposes of this Note are found in Justice Sotomayor's concurrence. After discussing why she believed the majority was correct, Justice Sotomayor added:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[131]

Just six years later, the Supreme Court had such an opportunity to consider Justice Sotomayor's suggestion.

---

124 David A. Harris, Riley v. California *and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 923 (2016).

125 *Riley*, 134 S. Ct. at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

126 *See* Harris, *supra* note 124, at 2495.

127 565 U.S. 400 (2012).

128 *See id.* at 403–04.

129 *See id.* at 403.

130 *See id.* at 404–06.

131 *Id.* at 417–18 (Sotomayor, J., concurring) (citations omitted).

IV. *CARPENTER V. UNITED STATES*: THE START OF A PRIVACY REVOLUTION?

As the previous Section describes, there are indications that the Supreme Court is ready to reconsider the foundations of some of its long-standing privacy decisions. In 2018, the Court did exactly that when it decided *Carpenter*. As the following Section discusses, *Carpenter* involved such a near-perfect data trail that the Supreme Court—consistent with Justice Sotomayor's concurrence in *Jones*—was forced to make changes in how Fourth Amendment law applies to the digital age. Despite the Court admonishing that the decision was narrow, it is very possible that the underlying principles of the decision—should Bitcoin ever obtain a similar type of complete data trail—will force the Court to expand its reasoning to other technologies. If that occurs, the federal government's primary anti-money laundering statute (the BSA) may be in constitutional jeopardy.

A. CSLI Data: A Near-Perfect and Accurate Data Trail

In 2018, the Supreme Court issued its long-anticipated *Carpenter* opinion—a decision that may just revolutionize Fourth Amendment law. The Court examined whether cell-site location information ("CSLI")—the "time-stamped record" a phone creates "[e]ach time the phone connects to a cell site"—should be governed by the long-standing third-party doctrine or *Katz*'s reasonable expectation of privacy standard.[132]

The petitioner, Timothy Carpenter, appealed his conviction for robbery and firearm possession in relation to several robberies committed in the Detroit, Michigan area.[133] Carpenter argued that the government's failure to use a warrant constituted a search and seizure in violation of the Fourth Amendment.[134] Both the district court and the U.S. Court of Appeals for the Sixth Circuit—applying the third-party doctrine—held that because the petitioner did not have "a reasonable expectation of privacy in the location information," the government did not need a warrant.[135]

In bringing the case, FBI officials issued two separate subpoenas for petitioner's CSLI data,[136] pursuant to the Stored Communications

---

132 138 S. Ct. 2206, 2211 (2018).

133 *See id.* at 2212–13.

134 *See id.* at 2213.

135 *Id.* at 2212–13.

136 *See id.* at 2235.

Act,[137] which allows requests that fall "well short of the probable cause required for a warrant."[138] The first covered more than 150 days' worth of CSLI data.[139] The second, which the FBI hoped would reveal Carpenter's movements over a seven-day period, only produced two days' worth of CSLI data.[140] Both subpoenas combined covered 12,898 data points.[141] Using these records, the government was able to place petitioner in the exact geographic area as the four robberies at the time they occurred—a fact that was critical to his conviction.[142]

This was no ordinary data. The CSLI data was so comprehensive and detailed that the Court described it "as if [the government] had attached an ankle monitor to the phone's user."[143] The majority expressed shock at the extent to which the data could reveal the petitioner's movements, writing:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[144]

Importantly, the data was not voluntarily shared by Carpenter in the traditional sense. The data was produced regardless of whether Carpenter turned his phone's "Location" feature on or off.[145] "Apart from disconnecting the phone from the network," the Court wrote, "there is no way to avoid leaving behind a trail of location data."[146]

B. The U.S. Supreme Court Charts a New Path Forward

Carpenter represents a new path forward from the bright-line rules of *Katz* and *Miller* and may be best described as a Court struggling to apply those cases to a new type of unique data. Recognizing the special nature of the data at hand, the majority concluded that the FBI's access to petitioner's cell phone location data was analogous to

---

137 Pub. L. No. 99-508, 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. §§ 2701–2712).

138 *Carpenter*, 138 S. Ct. at 2221.

139 *See id.* at 2212.

140 *See id.*

141 *See id.*

142 *See id.* at 2212–13.

143 *Id.* at 2218.

144 *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

145 *See Carpenter*, 138 S. Ct. at 2211.

146 *Id.* at 2220.

attaching a GPS to a vehicle,[147] which requires a warrant because the suspect possesses a reasonable expectation of privacy in his movements.[148] The data, according to the Court, was incredibly sensitive, allowing the government to track petitioner's "every movement" and revealing petitioner's "familial, political, professional, religious, and sexual associations."[149] Because the data was so comprehensive and permitted the government to "travel back in time to retrace a person's whereabouts," the Court believed some privacy protection was warranted.[150]

The Court also rejected the government's argument that Carpenter could not enjoy an expectation of privacy in this data because it was voluntarily shared with his cell phone carriers.[151] The tremendous change in technology since the days of *Miller* likely caused the Court to modify its longstanding holding. Carpenter's conveyance of his CSLI data was not really a conscious, voluntary choice because, like so many Americans, he could not realistically operate in modern life without using a cell phone and, by extension, sharing that data.[152] Additionally, after acknowledging the automatic generation of the data, the Court stated, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."[153] The "inescapable and automatic nature of [the data's] collection," therefore, led the Court to conclude it was in no sense shared or voluntary.[154]

Ultimately, the majority's analysis developed into what a dissenting Justice Kennedy identifies as a five-factor test for determining whether information is protected by the Fourth Amendment in a post-*Carpenter* world: the information's "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[155] Finding that the "unique nature of cell phone location records"[156] satisfies each of these factors, the Court held that the petitioner did, indeed, have an expectation of

147 *See id.* at 2216.

148 *See id.* at 2220 (citing *Jones*, 565 U.S. at 430). In contrast, however, the short-term tracking of an individual as he drives on public streets does not require a warrant.

149 *Id.* at 2215, 2217.

150 *Id.* at 2218.

151 *See id.* at 2220.

152 *See id.*

153 *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

154 *Id.* at 2223.

155 *Id.* at 2234 (Kennedy, J., dissenting).

156 *Id.* at 2217 (majority opinion).

privacy in the data.[157] The government's unwarranted search and seizure of that data, therefore, was unconstitutional.[158]

C. Carpenter*'s Impact on New Technologies Is Unclear*

Chief Justice Roberts's insistence that *Carpenter* is a narrow decision[159] speaks to the majority's recognition that the decision's principles have the potential to completely revolutionize Fourth Amendment privacy jurisprudence. Of course, this should be no surprise: legal commentators spent the months leading up to oral argument debating what the Court should do.[160] Other experts—carefully analyzing the Court's reasoning after the case was decided—focused on the decision's long-term impact.[161] One privacy law expert, Professor Orin Kerr, noted that *Carpenter* "recasts a lot of doctrine in ways that could be used to argue for lots of other changes."[162] He posits that the decision effectively places an "equilibrium-adjustment cap" on the third-party doctrine whereby the Court decides whether to expand or limit government surveillance in light of new technologies based on how those technologies can potentially invade privacy rights.[163] The cap set forth in *Carpenter*, Professor Kerr argues, draws a line where "the surveillance is just too much to allow, and at that point the third-party doctrine doesn't apply."[164] The Court does not answer the question of where exactly this line lies, says Professor Kerr, but the Court does list factors that will impact that determination, including the sensitivity, pervasiveness, and types of records involved.[165]

Others have echoed that sentiment, arguing that the majority's holding "seems to actually invite . . . litigation" despite its insistence

---

157 *See id.*

158 *See id.* at 2223.

159 *See id.* at 2220.

160 *See, e.g.*, Daniel Solove, *10 Reasons Why the Fourth Amendment Third Party Doctrine Should be Overruled in* Carpenter v. US, TeachPrivacy (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled/ [https://perma.cc/G7XG-WS7P] ("It is time for the Fourth Amendment to be rejuvenated and brought back to the forefront of managing our privacy in today's digital age.").

161 *See, e.g.*, Chuck Stanley, *Cell Data Privacy Ruling May Spawn Suit Avalanche, Attys Say*, Law360 (July 2, 2018, 8:18 PM), www.law360.com/articles/1059664/cell-data-privacy-ruling-may-spawn-suit-avalanche-attys-say [https://perma.cc/S5QX-WVXA].

162 Orin S. Kerr, *Initial Reactions to* Carpenter v. United States 4 (Univ. of S. Cal. Gould Sch. of Law, Legal Studies Paper No. 18-14, 2018), https://ssrn.com/abstract=3209587 [https://perma.cc/5P6V-7824].

163 *Id.* at 2, 4–5.

164 *Id.* at 5.

165 *Id.*

on narrowness.[166] In a very real sense, *Carpenter* may lead to many law enforcement searches requiring a warrant if the data can be characterized as revealing "an intimate window into a person's life," the exact opposite of the current legal landscape.[167] Future cases may stop asking whether the petitioner has a reasonable expectation of privacy. Judges may be more likely to inquire about the extent to which the data requested was just as revealing, comprehensive, and inescapably collected as the CSLI data sought in *Carpenter*, inquiries that may lead future courts to extend *Carpenter*'s reasoning to those records.[168]

Some have conducted extensive examinations into the majority's opinion but found no conclusive clues about how future cases may be resolved.[169] Others have argued that the majority's reasoning in *Carpenter* should make the privacy policies, practices, and disclosure agreements of third parties critical to the determination of whether the third-party doctrine applies.[170] One scholar has argued that sensitivity should be added to the Court's test, a factor that would then launch an investigation into whether a "mosaic" of the suspect can be created such that privacy rights should be extended to that situation.[171] But one thing is certain: *Carpenter* will undoubtedly have a lasting impact on Fourth Amendment law and is likely to be considered among the most significant privacy cases ever decided.

D. Are the BSA's Days of Covering Bitcoin Numbered?

As mentioned earlier, *Carpenter* appears to advance a multi-factor test for determining the law's treatment of new types of data made available only by modern technology: (1) intimacy, (2) comprehen-

166 Sarah Hall & Brian Lanciault, Carpenter *and the High Court's Shift on 4th Amendment*, Law360 (July 23, 2018, 1:22 PM), https://www.law360.com/articles/1065806/carpenter-and-the-high-court-s-shift-on-4th-amendment [https://perma.cc/5P6V-7824].

167 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); *see* John M. Burkoff, Search Warrant Law Deskbook §§ 3.1–3.2 (rev. ed. Feb. 2019); Matthew J. Gardner et al., *Internet of Things Cos. Must Prepare for Law Enforcement*, Wiley Rein LLP (Aug. 16, 2018), https://www.wileyrein.com/newsroom-articles-Internet-Of-Things-Cos-Must-Prepare-For-Law-Enforcement.html [https://perma.cc/K52J-LLFJ] ("Although Carpenter dealt with a specific category of data . . . it is unclear how the Supreme Court's expansion of Fourth Amendment privacy protections will impact other categories of data.").

168 *See* Nameir Abbas et al., Carpenter *Ruling May Be Turning Point in Digital Data Privacy*, Alston & Bird (Aug. 8, 2018), https://www.alston.com/en/insights/publications/2018/08/carpenter-ruling-may-be-turning-point [https://perma.cc/896M-V5SM].

169 *See, e.g.*, Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 Sup. Ct. Rev. 411, 416 (2019).

170 *See, e.g.*, Ram, *supra* note 6, at 20–22.

171 *See* Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 Ga. L. Rev. 1039, 1046 (2019).

siveness, (3) expense, (4) retrospectivity, and (5) voluntariness.[172] The third-party doctrine, which has long governed privacy interests in business records, now appears to be just one factor among many a court should weigh in situations not governed by *Miller* or *Smith*.

Like CSLI data, Bitcoin is a new type of information that will challenge the Court's longstanding application of Fourth Amendment protections in the context of data that may not be strictly classified as business records. As the majority stated, "the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[173] There is a real possibility that the Court's fifth factor may be outweighed by the other four, a scenario that triggers Fourth Amendment protection for Bitcoin records.

1. Intimacy

First, Bitcoin is most certainly capable of providing data that, like CSLI data, reveals the intimacies of an individual user's life. It has a popular reputation for being anonymous[174] but operates pseudonymously in practice.[175] Remember, Bitcoin's underlying algorithm is just a "string of letters and numbers"[176] that instructs the Bitcoin ecosystem how to transfer coins across accounts, each of which have their own, unique identifying code.[177] Transaction history is recorded on each ledger connected to the Bitcoin network and is publicly available for any user to see.[178] Bitcoin's use of encryption and lack of a single central entity may make it more difficult to reveal a user's true identity or manipulate transaction data, but that does not mean the task is impossible. Cryptocurrency exchanges, where users buy and sell different cryptocurrencies to each other, including Bitcoin, have already been hacked, allowing nefarious actors to steal millions in value.[179] Researchers at the University of Qatar recently published a report in which they successfully reversed Bitcoin transaction history

172 *See Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting).

173 *Id.* at 2223.

174 *See* Ducas & Wilner, *supra* note 46, at 545.

175 *See* Saman Jafari et al., *Cryptocurrency: A Challenge to Legal System* 11 (May 2, 2018) (unpublished manuscript) (available at https://ssrn.com/abstract=3172489 [https://perma.cc/B7G6-WBME]) (citing Steven Goldfeder et al., *When the Cookie Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies*, 2018 SCIENDO 179 (2017)).

176 Werbach, *supra* note 44.

177 *See* Tom W. Bell, *Copyrights, Privacy, and the Blockchain*, 42 OHIO N.U. L. REV. 439, 463 (2016) (describing the manner by which the blockchain, in the context of Bitcoin, records and transmits transaction data).

178 *See* Agrawal, *supra* note 48.

179 *See* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*,

to identify users' real-life identities.[180] This supposed "shield" of anonymity turns out to be no more anonymous than a user's cell phone data, and law enforcement has already succeeded in connecting suspect transactions to particular users.[181] As law enforcement agencies continue to exert jurisdiction over this new technology and become more familiar with exactly how users may conceal their activities on the Bitcoin network, connecting accounts with real-life identities will only become easier.[182] In fact, the mere identification of a user may produce a treasure trove of data, including where a user purchases coffee, where they send their children to school,[183] what restaurants they frequent,[184] what political parties the user is associated with,[185] what publications the user reads,[186] and even how much a user donates to his or her place of worship.[187] And as Bitcoin becomes more mainstream and users pay for more services using Bitcoin, this factor will

---

WIRED (Mar. 3, 2014, 6:30 AM), https://www.wired.com/2014/03/bitcoin-exchange/ [https://perma.cc/BU7B-EDCH].

180 Husam Al Jawaheri et al., *Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis* 9 (July 10, 2019) (unpublished manuscript) (available at https://arxiv.org/pdf/1801.07501.pdf [https://perma.cc/5FVM-PNDF]) ("The main security implication of our work is that . . . Bitcoin addresses can be exploited to deanonymize users.").

181 *See* Russell Brandom, *Feds Ran a Bitcoin-Laundering Sting for over a Year*, VERGE (June 27, 2018, 1:44 PM), https://www.theverge.com/2018/6/27/17509444/dark-web-drug-market-money-laundering-hsi-dark-gold [https://perma.cc/QXR4-PL7X].

182 *See* Godlove, *supra* note 43, at 11 ("[L]aw enforcement will soon be able to identify likely targets whom they suspect of illegally using virtual currency. Furthermore, identification will be retrospective, meaning that someone who bought drugs on Silk Road in 2011 will still be identifiable on the basis of the block chain whenever these techniques are developed. These deanonymization techniques are well known to computer scientists, and therefore to the [National Security Agency], and likely eventually will be used by law enforcement.").

183 *See* Noah Hurowitz, *Where Can I Actually Spend Bitcoin in New York City?*, N.Y. MAG. (Dec. 26, 2017), http://nymag.com/intelligencer/2017/12/businesses-in-new-york-that-accept-bitcoin.html [https://perma.cc/7YP7-4RSG].

184 *See Fast Food Restaurants that Accept Bitcoin in United States*, SPENDBITCOINS, http://spendbitcoins.com/places/c/fast-food/ [https://perma.cc/75D2-QWS7].

185 *See* Ofir Beigel, *Who Accepts Bitcoin as Payment?*, 99BITCOINS (Nov. 12, 2019) https://99bitcoins.com/bitcoin/who-accepts/ [https://perma.cc/4E2N-3J3V].

186 *See id.*

187 *See* Anthony Cuthbertson, *London Mosque Becomes First to Accept Cryptocurrency After Bitcoin Declared Halal*, INDEPENDENT (May 23, 2018, 11:58 AM), https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-halal-london-mosque-donations-cryptocurrency-islam-sharia-law-muslim-ramadan-zakat-a8364846.html [https://perma.cc/6VZN-B5QK]; Cristina Maza, *Bitcoin Now Accepted as Church Offering in Switzerland Despite Fears of Cryptocurrency Bubble*, NEWSWEEK (Jan. 18, 2018, 9:34 AM), https://www.newsweek.com/bitcoin-accepted-church-offering-784354 [https://perma.cc/E5AA-7T5L]; *see also* Fernando Alfonso III, *How Mt. Gox Scared Off the First and Only Bitcoin Synagogue*, DAILY DOT (Feb. 25, 2017, 1:05 AM), https://www.dailydot.com/business/bitcoin-synagogue-mt-gox/ [https://perma.cc/HZ6U-8WX7] (reporting that a Baltimore synagogue embraced and subsequently rejected Bitcoin as a way to accept donations).

only grow in importance. Bitcoin users, in a very real sense, will be at risk of exposing the intimacies of their life to anyone capable of identifying their wallets.

2. Comprehensiveness

Second, Bitcoin's structure collects and permanently records a comprehensive list of every transaction in which a particular user participated.[188] As discussed earlier, Bitcoin is a peer-to-peer network that relies on a network of decentralized ledgers to record and facilitate transactions.[189] Each transaction is irreversibly cataloged, and a single user can access the entire transaction history for any other account.[190] Imagine if Carpenter's CSLI data not only cataloged his movements but was also an access point for the government to obtain movements of every cell phone connected to Sprint's phone network. That is the incredible power and value of Bitcoin's network and the data it permanently and irreversibly stores.

3. Expense

Third, like the CSLI data in *Carpenter*, the government's projected expense in obtaining this data is low. Federal authorities, including FinCEN, have already been using the BSA to bring cryptocurrency exchanges, which allow users to buy and sell cryptocurrencies for cash or to exchange cryptocurrencies with each other,[191] under the BSA's purview.[192] As discussed earlier, Bitcoin's ledger system contains an incredibly detailed record of each wallet's transaction history.[193] Federal authorities, using their authority under the BSA, will have access to this near perfect record of a user's activity.[194] More importantly, however, application of the BSA to cryptocurrency exchanges will reduce federal authorities' expense in identifying individual users' real-world identity and obtaining person-

188 *See* Sumit Agarwal, Note, *Bitcoin Transactions: A Bit of Financial Privacy*, 35 CARDOZO ARTS & ENT. L.J. 153, 160 (2016).

189 *See* Sarah Gruber, Note, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32 QUINNIPIAC L. REV. 135, 145 (2013) (citing *How Bitcoin Works*, BITCOIN WIKI (Feb. 4, 2018, 7:36 AM), https://en.bitcoin.it/wiki/How_bitcoin_works [https://perma.cc/H5QK-YNY3]) (discussing how Bitcoin's encryption feature provides a measure of privacy, but see the prior paragraph for an explanation of why Bitcoin is not private in practice).

190 *See* Werbach, *supra* note 44, at 544–45.

191 *See* U.S. Dep't of Justice, *supra* note 19.

192 *See* FinCEN, *supra* note 18.

193 *See supra* Section I.B.

194 *See supra* notes 183–89 and accompanying text.

ally identifying information. Cryptocurrency exchanges often require new users to include personal information when opening an exchange account, which means the exchange not only has access to an individual Bitcoin user's wallet but also the real-life identity of that wallet's user.[195] The government, relying on its authority under the BSA, will now have easy access to public Bitcoin data and users' private information, all of it contained in the BSA's reports, which the exchanges submit to federal authorities. If an exchange user ties multiple wallets to his exchange account, the government has an even clearer picture of his Bitcoin activities.

Furthermore, the treasure trove of data federal authorities will receive from these reports may enable the government to deanonymize nonexchange Bitcoin profiles. In 2019, a group of researchers from Qatar University examined whether public Bitcoin data could be used to reveal the identities of users on an anonymous, deep-web internet browser called "Tor."[196] By tracking flows of transactions in and out of accounts, surveying social media profiles, and cross-matching Bitcoin public addresses with Tor user profiles, the researchers were able to deanonymize individual users.[197] Researchers were able to determine one user was a "middle aged man from Sweden," and that the other 22 users included "four males and six females of different ages that range between 13 and 42 years [old]."[198]

While the researchers noted that employing their methodology alone would likely only lead to a small number of users being deanonymized, they suggested that combining their techniques with successful efforts by other researchers could reveal the profiles of a much broader number of users.[199] One study they cited, which employed "behavior-based clustering" of Bitcoin user profiles, was able to deanonymize 40% of Bitcoin users simply by examining spending habits and time zone data.[200] Another study was successful in identifying Bitcoin users despite those users' reliance on mixing services, which seek to divide Bitcoin transactions into smaller payments to frustrate any attempts to retroactively identify users.[201]

---

195 *See* EDWARD V. MURPHY ET AL., CONG. RESEARCH SERV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 3 (2015).

196 *See* Jawaheri et al., *supra* note 180, at 1.

197 *See id.* at 8–9 ("The main security implication of our work is that a Bitcoin address[ ] can be exploited to deanonymize users.").

198 *Id.* at 7–8.

199 *See id.* at 8–9.

200 *Id.* at 10.

201 *See id.* at 9.

The government's ability to access personally identifying information contained in cryptocurrency exchange data, considering these academic studies, will dramatically reduce the burden federal authorities face in determining user identities. Like the Qatar University study, federal authorities may be able to use cryptocurrency exchange data to de-anonymize Bitcoin wallets that have never participated in an exchange.[202] In short, the personally identifying information contained in cryptocurrency exchange reports may be a gold mine law enforcement can use to identify users across the Bitcoin network.

4. Retrospectivity

Fourth, despite its inherent decentralization, Bitcoin's very structure allows for retroactive access. Records of transactions are constantly being copied across computers connected to the Bitcoin ecosystem such that each individual terminal contains a complete record of transaction data.[203] Practically, this means each and every Bitcoin network access point contains a potentially full picture of the entire network's history,[204] an even more comprehensive data set than the CSLI data in *Carpenter*. All the government would need to do to access that data is identify an account and decrypt the history of transactions associated with that account.[205] Like *Carpenter*, this presents an easy way for the government to access a user's full history. Law enforcement would not need to carefully and affirmatively assemble a user's history; Bitcoin does that itself.

5. Voluntariness

Finally, the new *Carpenter* test deals with the extent to which a user voluntarily shares data with a third party. Critical to the Court's holding was the fact that the CLSI data in question was not "shared" by Carpenter in the traditional sense. Carpenter could not avoid sharing this data apart from keeping his phone off, and any activity on the phone automatically generated CLSI data.[206] In short, Carpenter had "no way to avoid leaving behind a trail of location data."[207]

---

202 *Id.* at 10 ("Our results has [sic] one immediate implication: Bitcoin addresses should always be assumed compromised as they can be used to deanonymize users.").

203 *See* Gruber, *supra* note 189, at 147, 164 (explaining how Bitcoin operates on a "blockchain" whereby software is constantly updating itself to reflect transaction history across terminals, also known as "nodes").

204 *See* Godlove, *supra* note 43, at 11.

205 *See* Agarwal, *supra* note 188, at 160.

206 *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

207 *Id.*

At the time of this Note's writing, Bitcoin is, concededly, not such a "pervasive and insistent part of daily life" that a user is able to avoid disclosing the type of comprehensive and intimate data the network gathers.[208] Users can use cash, credit cards, or some other third-party payment system to avoid dissemination of their data across a distributed ledger system. This reality would likely lead a court to find that Bitcoin usage—at this time—does not qualify as the type of "inescapable and automatic" data collection present in *Carpenter*.[209] Nevertheless, it is conceivable that Bitcoin could become such a dominant part of life that this factor weighs in favor of Fourth Amendment protection, should Americans one day rely on Bitcoin for most or even a significant portion of their financial transactions. And if a non-Bitcoin form of blockchain ever becomes fully integrated into existing payment systems, that network may trigger the type of widespread and automatic data collection scheme at issue in *Carpenter*.

Despite the fifth factor currently weighing against a Fourth Amendment privacy interest in Bitcoin, a court may nonetheless determine that the other four factors are strong enough to grant it Fourth Amendment protections. As Professor Kerr has noted, Chief Justice Roberts's majority opinion contains language that leaves the possibility of *Carpenter*'s extension in the future, despite the Court's language about a narrow holding.[210] Professor Kerr calls this "equilibrium-adjustment," and it appears to provide enough flexibility for a court to rebalance privacy interests in light of new and intrusive technologies.

In *Carpenter*, the Chief Justice is very clear that the Court is engaging in equilibrium-adjustment. Throughout the opinion, he roots his analysis in the idea that cell-site surveillance is a new tool that gives the government new power that can be abused, and that the law must change course to ensure that the government doesn't get too much power from a mechanical application of the old rules.[211]

It is possible that a future Supreme Court—recognizing the power that the Bitcoin network and its underlying technology gives a government investigator in recreating a user's entire history—will find such equilibrium-adjustment appealing. The mere possibility of that

---

208 Riley v. California, 134 S. Ct. 2473, 2484 (2014).

209 *Carpenter*, 138 S. Ct. at 2223.

210 *See* Kerr, *supra* note 162, at 2, 4–5.

211 *See* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/Q5XS-KNHV].

finding means that the BSA's authorization of warrantless data collection in the context of financial records may be at risk. As detailed above, the BSA serves as the very core of the federal government's AML, counterterrorist financing, and other financial crimes enforcement network. Declaring the BSA unconstitutional as applied to Bitcoin would put that regime in jeopardy. In such a decision, the failure to properly delineate publicly available data from encrypted, privately identifying information, could dramatically curtail the government's ability to combat illicit activities on the network, especially if a court considers even the publicly available information—due to its intimacy, comprehensiveness, retroactivity, and low expense—to be protected by the Fourth Amendment.

E. What Happens If the Bank Secrecy Act Is Struck Down?

A successful constitutional challenge to the BSA's reporting and recordkeeping regime as applied to Bitcoin poses serious problems for the federal government's efforts to combat financial crimes. Nefarious actors, who have already used Bitcoin's network to try and extort American politicians[212] and conduct illegal sales of guns and drugs online,[213] would likely find the network an even more attractive venue for their unlawful activities. Terrorists, arms dealers, and money launderers would flock to and fully exploit the network to avoid the chance of prosecution. The average American, of course, would still have his or her non-Bitcoin activities—mainly banking and other financial transaction information—scrutinized by federal regulators under the BSA. But the very type of activity the BSA was designed to prohibit would migrate to this new, unregulated area of cyberspace and beyond the government's reach.

A cursory glance at FinCEN's website provides a brief overview of the types of investigations that would be in jeopardy. Crimes including money laundering, casino fraud, terrorism, insurance fraud, and the narcotics trade would be much easier to conduct.[214] FinCEN's ability to investigate the illicit transfer of funds to rogue regimes like Iran might be impacted.[215]

---

212 *See* Gruber, *supra* note 189, 135–39.

213 *See id.* at 156.

214 *See Investigations Assisted by Bank Secrecy Act Data*, FinCEN, https://www.FinCEN.gov/investigations-assisted-bank-secrecy-act-data [https://perma.cc/SU7D-EYHE].

215 *See SAR Initiatives Investigation of Illegal Money Transfers to Iran*, SAR Activity Rev., Feb. 2003, at 51; *see also Post 9/11 SAR Leads to Guilty Plea in Money Laundering and Illegal Transfer of Funds to Iran Investigation*, SAR Activity Rev., May 2007, at 27–28.

Domestic crimes that touch average Americans, such as real estate fraud rings[216] or telemarketing scams,[217] would also be more difficult to identify and prosecute. Likewise, the federal government's ability to combat organized crime—the very purpose for which the BSA was passed—would also erode.[218] In short, current and future investigations would suddenly be thrown into flux. Defendants could challenge their indictments on the basis that the evidence against them was seized in violation of the Fourth Amendment, and law enforcement's ability to quickly identify, investigate, and prosecute future crimes such as the ones listed above would be dramatically curtailed.

V. Congress Should Amend the Bank Secrecy Act, Extending its Coverage to Bitcoin

As described in Section II.A, the BSA creates a comprehensive reporting and recordkeeping regime[219] designed to facilitate enforcement of AML and other federal financial crime laws.[220] By creating a paper trail of suspicious transactions and accounts, the BSA's writers hoped law enforcement could more easily discover nefarious activity within the banking system.[221]

The BSA's process by which a government agency can access these records is described as follows:

> Except as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and—
> (1) such customer has authorized such disclosure in accordance with section 3404 of this title;

---

216 *See Bank Secrecy Act Reports Instrumental in Investigation and Conviction of Attorney and Three Accomplices in Multi-Million Dollar Real Estate Fraud*, SAR Activity Rev., Aug. 2004, at 35.

217 *See Suspicious Activity Reports Assist Telemarketing Fraud Investigation*, SAR Activity Rev., Aug. 2004, at 33–34.

218 *See, e.g.*, *BSA Records "Critical" in Conviction of Money Launderer in Organized Retail Theft Case*, SAR Activity Rev.: Trends, Tips & Issues, Oct. 2008, at 27–28; *Organized Crime Network Attacked With the Help of SARs*, SAR Activity Rev.: Trends, Tips & Issues, Oct. 2000, at 18.

219 *See supra* Part II.A.

220 *See* 31 U.S.C. § 5311 (2012) ("It is the purpose of this subchapter (except section 5315) to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities.").

221 *See* H.R. Rep. No. 91-975, at 10, 15–16 (1970).

> (2) such financial records are disclosed in response to an administrative subpena [sic] or summons which meets the requirements of section 3405 of this title;
> (3) such financial records are disclosed in response to a search warrant which meets the requirements of section 3406 of this title;
> (4) such financial records are disclosed in response to a judicial subpena [sic] which meets the requirements of section 3407 of this title; or
> (5) such financial records are disclosed in response to a formal written request which meets the requirements of section 3408 of this title.[222]

To ensure that the BSA as applied to Bitcoin survives any potential *Carpenter*-type challenge, Congress ought to amend 12 U.S.C. § 3402 to require a warrant where personally identifying information is sought. Anonymous data (e.g., the type of encrypted and non-identifying transaction history that any Bitcoin user can view) should continue to be accessible via a subpoena or written request. To that end, section 3402 ought to be amended as follows:

> Except as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and—
> (1) such customer has authorized such disclosure in accordance with section 3404 of this title;
> (2) **in the context of anonymous data or transaction history**, such financial records are disclosed in response to an administrative subpena [sic] or summons which meets the requirements of section 3405 of this title**, provided that the records disclosed do not contain personally identifying information**;
> (3) such financial records are disclosed in response to a search warrant which meets the requirements of section 3406 of this title;
> (4) **in the context of anonymous data or transaction history,** such financial records are disclosed in response to a judicial subpena [sic] which meets the requirements of section 3407 of this title, **provided that the records disclosed do not contain personally identifying information**; or
> (5) **in the context of anonymous data or transaction history,** such financial records are disclosed in response to a for-

222 12 U.S.C. § 3402 (2012).

> mal written request which meets the requirements of section 3408 of this title**, provided that the records disclosed do not contain personally identifying information**.

Because the term "personally identifying information" is inherently ambiguous, Congress ought to also amend 12 U.S.C. § 3401—which defines § 3402—to include the following text:

> (9) "personally identifying information," with respect to financial records sought under this chapter, refers to the user's identify, name, address, social security number, and other identifying information, but does not include an anonymous IP address, encrypted account identity, or other anonymous data or transaction history that, without additional information, shields a user's identity.

These modifications to the BSA's reporting regime should satisfy the Court's new privacy test under *Carpenter*. Highly detailed information that reveals "an intimate window into a person's life" will receive heightened privacy protections by statute.

Concerns that these changes will limit law enforcement's ability to conduct investigations are not well founded because these changes will not prohibit generalized surveillance or record monitoring under the BSA. With today's technology, anonymous data points associated with the same accounts or group of accounts can reveal a tremendous amount of information.[223] Law enforcement would still be able to gather and study publicly available transaction history indicating that a particular Bitcoin *user* was engaging in a pattern of transactions that is suggestive of money laundering or some other crime. The only thing that law enforcement could not obtain without a warrant would be the user's *identity*. And as law enforcement officers use this public transaction data to find incriminating evidence, a warrant for the user's identity should not be difficult to obtain. In short, these changes simply require that when a law enforcement agency seeks to move beyond the *surveillance* stage and actually identify a particular individual, entity, or group, it must obtain a warrant.[224] These types of

---

223 *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, 38 ;LOGIN: 10, 14 (2013) ("By layering this clustering analysis on top of our ground-truth data . . . we were able to identify 1.9 million public [Bitcoin] keys with some real-world service or identity . . . . Although this is a somewhat small fraction (about 16%) of all public keys, it nevertheless allows us to deanonymize significant flows of bitcoins throughout the network.").

224 *See* Carrie Kirby, *Following the Money: Researcher Tracks Bitcoin Movements and Anonymity*, COINDESK (Jan. 13, 2014, 1:23 PM), https://www.coindesk.com/researcher-tracks-bitcoin-movements-anonymity [https://perma.cc/9TQP-4CJP?type=image] ("[U]ltimately the fact that

investigations are often not particularly time-sensitive, and the limited warrant requirement is a relatively small burden on law enforcement.

Conclusion

The 21st century has seen and will continue to see new technologies that present possible challenges to longstanding Fourth Amendment jurisprudence. The Supreme Court's *Carpenter* decision has the potential to fundamentally and permanently alter how courts view Fourth Amendment privacy protections in the digital age. Although a narrow decision, the Court's reasoning presents a new way to balance the individual right to privacy with the government's ability to access personally revealing information that is critical to enforcing criminal laws.

Bitcoin—and cryptocurrency in general—presents a possible avenue by which a constitutional challenge can be levied against the BSA, the federal government's primary AML and anti-terrorist financing law. *Carpenter* raises sufficient doubt about the constitutionality of the BSA as applied to Bitcoin such that Congress should proactively amend the BSA to bring it in line with *Carpenter*'s reasoning. Even without a current challenge, law enforcement may be much less willing to conduct investigations without a warrant out of fear that evidence may be challenged as an unconstitutional violation of the Fourth Amendment.

To resolve this doubt and ensure law enforcement continues to have access to the tools it needs to combat money laundering, terrorist financing, and other financial crimes, Congress ought to amend the BSA to require a warrant when law enforcement seeks personally identifying information. Anonymous data points and public transaction history stored on the Bitcoin network will remain subject to the BSA's subpoena and written request procedures. However, to ensure law enforcement can uncover nefarious financial activity while bolstering Americans' privacy interests, the BSA ought to require a higher threshold for accessing more sensitive data. In this way, Congress can help the *Carpenter* majority realize its goal of a narrow and limited holding.

---

every transaction was publicly available was going to shoot you in the foot when you try to obscure the flow of large amounts of bitcoins.").