IN THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

United States Court of Appeals
Fifth Circuit
FILED
June 30, 2020
Lyle W. Cayce
Clerk

No. 19-50492

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

RICHARD NIKOLAI GRATKOWSKI,

Defendant - Appellant

Appeal from the United States District Court
for the Western District of Texas

Before STEWART, DENNIS, and HAYNES, Circuit Judges.

HAYNES, Circuit Judge:

Richard Gratkowski appeals the district court's denial of his motion to suppress evidence obtained through a search warrant. We AFFIRM.

I. Background

A. Factual Background

Gratkowski became the subject of a federal investigation when federal agents began investigating a child-pornography website (the "Website").[1] To

[1] The actual name of the Website remained confidential during the district court proceedings in light of an ongoing investigation. We continue to use this generic name.

download material from the Website, some users, like Gratkowski, paid the Website in Bitcoin.

Bitcoin is a type of virtual currency. Each Bitcoin user has at least one "address," similar to a bank account number, that is a long string of letters and numbers. Bitcoin users send Bitcoin to other users through these addresses using a private key function that authorizes the payments. To conduct Bitcoin transactions, Bitcoin users must either download Bitcoin's specialized software or use a virtual currency exchange, such as the one used here, called Coinbase.

When a Bitcoin user transfers Bitcoin to another address, the sender transmits a transaction announcement on Bitcoin's public network, known as a blockchain.[2] The Bitcoin blockchain contains only the sender's address, the receiver's address, and the amount of Bitcoin transferred. The owners of the addresses are anonymous on the Bitcoin blockchain, but it is possible to discover the owner of a Bitcoin address by analyzing the blockchain.

For example, when an organization creates multiple Bitcoin addresses, it will often combine its Bitcoin addresses into a separate, central Bitcoin address (i.e., a "cluster"). It is possible to identify a "cluster" of Bitcoin addresses held by one organization by analyzing the Bitcoin blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction.

---

[2] Blockchain is a technological advancement that permits members in a shared network to "record a history of transactions on an immutable ledger." *See* Ashley N. Longman, Note, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 118–19 (2019) (citing Brittany Manchisi, *What is Blockchain Technology?*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (July 31, 2018), https://www.ibm.com/blogs/blockchain/2018/07/what-is-blockchain-technology/).

B. Procedural History

Federal agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the Website. Once they identified the Website's Bitcoin addresses, agents served a grand jury subpoena on Coinbase—rather than seeking and obtaining a warrant—for all information on the Coinbase customers whose accounts had sent Bitcoin to any of the addresses in the Website's cluster. Coinbase identified Gratkowski as one of these customers. With this information, agents obtained a search warrant for Gratkowski's house. At his house, agents found a hard drive containing child pornography, and Gratkowski admitted to being a Website customer.

The Government charged Gratkowski with one count of receiving child pornography and one count of accessing websites with intent to view child pornography. Gratkowski moved to suppress the evidence obtained through the warrant, arguing that the subpoena to Coinbase and the blockchain analysis violated the Fourth Amendment. The district court denied the motion. Gratkowski entered a conditional guilty plea to both counts, reserving the right to appeal the denial of his motion to suppress. After the district court issued its final judgment, Gratkowski timely appealed.

II. Standard of Review

In reviewing "a district court's ruling on a motion to suppress, we review questions of law de novo and factual findings for clear error." *United States v. Ganzer*, 922 F.3d 579, 583 (5th Cir.), *cert. denied*, 140 S. Ct. 276 (2019) (mem.) (internal quotation marks and citation omitted). "We will uphold a district court's denial of a suppression motion if there is any reasonable view of the evidence to support [the denial]." *Id.* (internal quotation marks and citation omitted).

III. Discussion

Gratkowski presents the novel question of whether an individual has a Fourth Amendment privacy interest in the records of their Bitcoin transactions.[3] For the Government to have infringed upon an individual's Fourth Amendment protection against unreasonable searches, the person must have had a "reasonable expectation of privacy" in the items at issue. *United States v. Jones*, 565 U.S. 400, 406 (2012). Under the third-party doctrine, a person generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). But relying on *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), which limited the applicability of the third-party doctrine in the context of cell phones, Gratkowski argues that the Government violated his reasonable expectation of privacy in the records of his Bitcoin transactions on (1) Bitcoin's public blockchain and (2) Coinbase. In that regard, Gratkowski argues that the district court erred in denying his suppression motion. We hold that it did not.

A. The Third-Party Doctrine

Applying the third-party doctrine, the Supreme Court in *United States v. Miller* held that bank records were not subject to Fourth Amendment protections. 425 U.S. 435, 439–40 (1976). The Court concluded that the bank records were "not confidential communications but negotiable instruments," which "contain[ed] only information voluntarily conveyed to the banks and

[3] So far, we have found only two other federal district courts (and no circuit courts) that have addressed the issue of whether an individual has a privacy interest in the records of their Bitcoin transactions on a virtual currency exchange. *See Zietzke v. United States* (*Zietzke II*), No. 19-cv-03761, 2020 WL 264394 (N.D. Cal. Jan. 17, 2020); *Zietzke v. United States* (*Zietzke I*), 426 F. Supp. 3d 758 (W.D. Wash. 2019). In each case, the district court held that the defendant did not have a privacy interest in their Bitcoin transaction records because the transactions were shared with a third party, the virtual currency exchange. *Zietzke II*, 2020 WL 264394, at *13; *Zietzke I*, 426 F. Supp. 3d at 768-69.

exposed to their employees in the ordinary course of business." *Id.* at 442. It recognized that in enacting the Bank Secrecy Act, Congress assumed that individuals lacked "any legitimate expectation of privacy concerning the information kept in bank records." *Id.* at 442–43 (noting that the express purpose of the Act was "to require records to be maintained because they 'have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings'" (quoting 12 U.S.C. § 1829b(a)(1)).

The Court has also held that the third-party doctrine applies to telephone call logs. *Smith*, 442 U.S. at 742–44. It held that individuals had no privacy interest in the telephone numbers they dialed because people generally do not have any actual expectation of such privacy and "voluntarily convey[]" the dialed numbers to the phone company by placing a call. *Id.*

However, the Supreme Court recently concluded differently in the context of cell phones. *See Carpenter*, 138 S. Ct. at 2217. In *Carpenter*, the Court held that individuals had a privacy interest in their cell phone location records, known as cell-site location information ("CSLI"), despite the records being held by a third party. *Id.* In discussing the third-party doctrine, the Court noted that the sole act of sharing did not eliminate an individual's privacy interest. *Id.* at 2219. Rather, the Court considered (1) "the nature of the particular documents sought," which includes whether the sought information was limited and meant to be confidential, and (2) the voluntariness of the exposure. *Id.* at 2219–20 (internal citation and quotation marks omitted).

Regarding the nature of the information sought, the Court noted that "telephone call logs reveal little in the way of identifying information" and that checks are "not confidential communications but negotiable instruments . . . used in commercial transactions." *Id.* at 2219 (internal quotation marks and citations omitted). Unlike telephone call and bank records, CSLI

provides officers with "an all-encompassing record of the holder's whereabouts" and "provides an intimate window into a person's life, revealing not only [an individual's] particular movements, but through them [their] familial, political, professional, religious, and sexual associations." *Id.* at 2217 (internal quotation marks and citation omitted). Because individuals "compulsively carry cell phones with them all the time[,]" cell phones have become "almost a feature of human anatomy." *Id.* at 2218 (internal quotation marks and citation omitted). Thus, the Court held that CSLI "implicate[d] privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 2220.

As for the voluntary exposure component, the Court noted that CSLI was not voluntarily shared information for two reasons. First, "cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." *Id.* (internal quotation marks and citation omitted). Second, CSLI does not require "any affirmative act on the part of the user." *Id.* So long as the user has their cell phone on, a third party receives CSLI. *Id.*

B. Gratkowski's Reasonable Expectation of Privacy in his Information on the Bitcoin Blockchain

Gratkowski cites *Carpenter* to support his argument that he had a privacy interest in the information held in the Bitcoin blockchain. But the information on Bitcoin's blockchain is far more analogous to the bank records in *Miller* and the telephone call logs in *Smith* than the CSLI in *Carpenter*.

The nature of the information on the Bitcoin blockchain and the voluntariness of the exposure weigh heavily against finding a privacy interest in an individual's information on the Bitcoin blockchain. The Bitcoin blockchain records (1) the amount of Bitcoin transferred, (2) the Bitcoin address of the sending party, and (3) the Bitcoin address of the receiving

party. The information is limited. Moreover, transacting through Bitcoin is not "a pervasive [or] insistent part of daily life,"[4] and transferring and receiving Bitcoin requires an "affirmative act" by the Bitcoin address holder. *See Carpenter*, 138 S. Ct. at 2220 (internal citation and quotation marks omitted).

Further, Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private, thus undercutting their claim of a "legitimate expectation of privacy." *See Smith*, 442 U.S. at 743. Granted, they enjoy a greater degree of privacy than those who use other money-transfer means, but it is well known that each Bitcoin transaction is recorded in a publicly available blockchain.[5] Every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers. Due to this publicity, it is possible to determine the identities of Bitcoin address owners by analyzing the blockchain.[6] Gratkowski thus lacked a privacy interest in his information on the Bitcoin blockchain.[7]

---

[4] Unlike cell phones that are ubiquitous, Gratkowski points to nothing that suggests Bitcoin is central to most people's daily lives.

[5] *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2 (2008), https://bitcoin.org/bitcoin.pdf [hereinafter Nakamoto] (stating that Bitcoin transactions will be verified with a public system that records Bitcoin transaction histories).

[6] *See id.* at 6.

[7] Because we hold that there is no privacy interest in information stored in the Bitcoin blockchain, Gratkowski's argument—that the federal agents' method of using a "powerful and sophisticated software" to analyze the Bitcoin blockchain intruded into a constitutionally protected area and violated the Fourth Amendment—lacks merit. There is no intrusion into a constitutionally protected area because there is no constitutional privacy interest in the information on the blockchain.

C. Gratkowski's Reasonable Expectation of Privacy in his Bitcoin Transactions on Coinbase

Gratkowski again cites *Carpenter* to support his argument that he had a reasonable expectation of privacy in the Coinbase records that documented his Bitcoin transactions. Like the Blockchain, we hold that the Coinbase records are more akin to the bank records in *Miller* than the CSLI in *Carpenter*.

Coinbase is a financial institution, a virtual currency exchange, that provides Bitcoin users with a method for transferring Bitcoin. The main difference between Coinbase and traditional banks, which were at issue in *Miller*, is that Coinbase deals with virtual currency while traditional banks deal with physical currency. But both are subject to the Bank Secrecy Act as regulated financial institutions. *See Miller*, 425 U.S. at 440–41. Both keep records of customer identities and currency transactions. *See id.* at 437–38.

In that regard, the nature of the information and the voluntariness of the exposure weigh heavily against finding a privacy interest in Coinbase records. *See Carpenter*, 138 S. Ct. at 2219. First, Coinbase records are limited. Having access to Coinbase records does not provide agents with "an intimate window into a person's life"; it provides only information about a person's virtual currency transactions. *See id.* at 2217. Second, transacting Bitcoin through Coinbase or other virtual currency exchange institutions requires an "affirmative act on part of the user." *See id.* at 2220. Bitcoin users have the option to maintain a high level of privacy by transacting without a third-party intermediary. But that requires technical expertise, so Bitcoin users may elect to sacrifice some privacy by transacting through an intermediary such as Coinbase. Gratkowski thus lacked a privacy interest in the records of his Bitcoin transactions on Coinbase.

IV. Conclusion

For the foregoing reasons, we AFFIRM the district court's denial of Gratkowski's motion to suppress.[8]

[8] Even if the Supreme Court were to extend *Carpenter* to Bitcoin transactions in the future, we would still affirm the district court in this case because the good-faith exception applies to bar suppression. *United States v. Molina-Isidoro*, 884 F.3d 287, 290 (5th Cir. 2018) (this exception applies when the agents "acted with the objectively reasonable belief that their actions did not violate the Fourth Amendment"). Gratkowski was arrested in January of 2018 before *Carpenter* was decided and, of course, no court had applied such reasoning to Bitcoin transactions at that time. Thus, in such a circumstance, we would agree with the district court's holding that the agents "had no way to know, prior to *Carpenter*, that there could be a reasonable expectation of privacy in records like the ones obtained here."