NORTON ROSE FULBRIGHT

Blockchain Law

A little less privacy: Cryptocurrency transactions under the fourth amendment

Robert A. Schwinger, *New York Law Journal* — July 28, 2020

In his Blockchain Law column, Robert Schwinger discusses the appeal of using cryptocurrencies like Bitcoin and its perception that they may offer greater privacy protections for financial transactions. But a recent federal appellate ruling in a Fourth Amendment case suggests this perception may not align with current legal reality.

For some, the appeal of using cryptocurrencies like Bitcoin includes the perception that they may offer greater privacy protections for financial transactions, including shielding them from law enforcement scrutiny. But a recent federal appellate ruling in a Fourth Amendment case suggests this perception may not align with current legal reality.

In *United States v. Gratkowski,* 2020 WL 3530575 (5th Cir. June 30, 2020), the U.S. Court of Appeals for the Fifth Circuit held that the government's warrantless search of a Bitcoin blockchain associated with a child-pornography website and the government's subpoena to the cryptocurrency exchange Coinbase did not violate the defendant's Fourth Amendment protections against unreasonable searches and seizures. The ruling—the first time a federal appeals court has addressed the constitutional protections implicated by the use of cryptocurrencies and information stored on public blockchains—stands as a warning that the expectation of greater privacy in cryptocurrency transactions may be unwarranted, especially where transaction-related information is voluntarily shared with third parties like a cryptocurrency exchange.

Background

In *Gratkowski*, federal agents investigating a child-pornography website determined that the website accepted payment in Bitcoin. After analyzing a publicly viewable Bitcoin blockchain, the agents identified a "cluster" of Bitcoin addresses (a separate central address into which an organization combines multiple addresses that it controls) that was controlled by the child-pornography website. Rather than seek a warrant, however, the agents served a grand jury subpoena on the cryptocurrency exchange Coinbase, seeking information about Coinbase customers who had paid the website in Bitcoin. Coinbase identified the defendant Gratkowski as one of these customers. The agents then used this information to obtain a search warrant for Gratkowski's house, where they found a hard drive containing multiple images of child pornography. Gratkowski also admitted to being a website customer.

Gratkowski was charged in a two-count indictment with receiving and accessing child pornography. He moved to suppress the evidence obtained through the search warrant, arguing that the preceding blockchain analysis and subpoena to Coinbase on which the warrant was based were themselves Fourth

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP.
Jacob Laksin, a senior associate in the commercial litigation group, assisted in the preparation of this article.

Amendment searches that required a warrant. The suppression motion raised the "novel" question of whether Gratkowski had a constitutionally protected interest in the records of his Bitcoin transactions on a cryptocurrency exchange.

The 'third-party doctrine'

The suppression question turned on the application of the "third-party doctrine" under the Fourth Amendment. 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) (no Fourth Amendment protection for telephone call log information); see also *United States v. Miller*, 425 U.S. 435, 442 (1976) (depositors have no protectable Fourth Amendment interest in their bank records). Where the person lacks a "reasonable expectation of privacy" in the particular items at issue, the Fourth Amendment's protections against unreasonable searches and seizures are not triggered.

This doctrine has come under increasing scrutiny in recent years, particularly as more and more routine life activities are conducted through electronic and online means that involve interactions with third parties. Notably, in a 2012 U.S. Supreme Court decision holding (on different grounds) that the warrantless use of a GPS tracking device planted on an automobile was a Fourth Amendment violation, Justice Sonia Sotomayor commented in a separate concurring opinion that:

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. e.g., *Smith*, 442 U.S., at 742; *United States v. Miller*, 425 U.S. 435, 443 (1976). 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.

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

Gratkowski argued that the third-party doctrine did not apply in his case, and that he had a reasonable expectation of privacy in the records of his Bitcoin transactions on Bitcoin's public blockchain and with Coinbase. In particular, Gratkowski relied on the Supreme Court's 2018 decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), a 5-4 decision that limited the applicability of the third-party doctrine in the context of cell phone location data. *Carpenter* held that individuals had a protected privacy interest in their cell phone location data, known as cell-site location information (CSLI), despite its disclosure to third parties like wireless carriers. Rejecting a "mechanical" application of the third-party doctrine, the court noted that the sole act of sharing information with a third-party did not eliminate an individual's privacy interest and that courts also should consider "the nature of the particular documents sought," including whether the sought information was limited and meant to be confidential, and whether the information was "voluntarily conveyed" to third parties.

After an initial ruling against Gratkowski on the privacy interest issue, the district court revisited the issue and held that Gratkowski had a reasonable expectation of privacy in his Coinbase account records and that the third-party doctrine did not apply. Nevertheless, the district court still denied Gratkowski's suppression motion based on the "good-faith exception" to the exclusionary rule, which provides that evidence need not be suppressed where government agents acted with an objectively reasonable belief that their actions did not violate the Fourth Amendment. Gratkowski appealed to the Fifth Circuit.

Like bank records or mobile data?

In addition to defending the application of the "good faith exception" in Gratkowski's case, the government argued that neither the federal agents' analysis of the public blockchain data nor their subpoena to Coinbase violated the Fourth Amendment under the third-party doctrine because Gratkowski had no reasonable expectation of privacy in Bitcoin's public blockchain or in Coinbase's records. The government argued that *Carpenter* should be cabined to its facts (cellphone location data), and that the more relevant Supreme Court precedent was *Miller*, where the Supreme Court held that depositors have no protectable Fourth Amendment interest in their bank records. *Miller* reasoned that the bank records (such as canceled checks, deposit slips, and monthly statements) were "not confidential communications but negotiable instruments," which "contained only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" and thus individuals lacked "any legitimate expectation of privacy concerning the information kept in bank records."

The Fifth Circuit affirmed the denial of Gratkowski's suppression motion. It rejected Gratkowski's argument that he had a privacy interest in the information held in the Bitcoin blockchain, holding that "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*." Invoking the rationales for the third-party doctrine considered in *Carpenter*, the court pointed to the "limited" nature of the information on the blockchain, such as the amount of bitcoin transferred and the Bitcoin addresses of the sender and the recipients. The court also emphasized the voluntariness of Gratkowski's disclosure, including his transfer of the bitcoin, observing that "Bitcoin users are unlikely to expect that the information published on the Bitcoin blockchain will be kept private" because the Bitcoin transactions are recorded in a public blockchain. All of these factors weighed "heavily" against the finding a privacy interest in information on the Bitcoin blockchain.

Applying the same reasoning, the court found that Gratkowski had no privacy interest in the record of his Coinbase transactions either, concluding that Coinbase records, like the Bitcoin blockchain, were more akin to the bank records in *Miller* than the CSLI in *Carpenter*. In the court's view, the "main difference" between Coinbase and a traditional brick-and-mortar bank was that Coinbase deals with virtual currency while traditional banks deal with physical currency. The court deemed that difference insignificant, since both virtual and traditional banks were subject to the same regulatory scrutiny as financial institutions, such as the Bank Secrecy Act, and maintained the same "limited" information concerning customer identities and transactions. The court also noted in a footnote that even if *Carpenter's* limitations on the third-party doctrine were to be extended to Bitcoin transactions, "we would still affirm the district court in this case because the good-faith exception applies to bar suppression."

A failure of analogy?

Gratkowski may be seen, in part, as a failure of analogy on the part of the defendant. Unimpressed by Gratkowski's reliance on *Carpenter*, the court discounted any meaningful similarity between the cryptocurrency transaction information sporadically recorded on a digital blockchain or in the records of a cryptocurrency exchange and cell phone location data, which provides a near-continuous record of a person's movements every minute of the day. Unlike cell phones, which the court noted (citing *Carpenter*) "are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society," no evidence was presented to suggest that "Bitcoin is central to most people's daily lives." The court also distinguished between a Bitcoin user engaging in the affirmative act of effecting currency transactions and cell phone users who passively make CSLI available to third parties simply by having their cellphones on.

A consistent view

Though *Gratkowski* is the first federal appellate court to consider whether individuals have a Fourth Amendment privacy interest in information on their public blockchain, its conclusion is consistent with those of the few lower federal courts that have addressed the issue to date. In another recent example, in *Zietzke v. United States*, 2020 WL 264394 (N.D. Cal. Jan. 17, 2020), the court denied a motion to quash an IRS summons to Coinbase seeking information relevant to the petitioner's federal tax liability. Applying the third-party doctrine, the court held that, because the petitioner voluntarily exposed this information to Coinbase, he had no reasonable expectation of privacy in the information. A Washington district court, relying on *Miller*, had previously found that an IRS summons issued to cryptocurrency exchange Bitstamp did not infringe this same petitioner's Fourth Amendment rights because he had no reasonable expectation of privacy in his Bitstamp records. See *Zietzke v. United States*, 426 F. Supp. 3d 758, 769 (W.D. Wash. 2019).

Conclusion

Future litigation will define the full scope of the privacy protections, if any, afforded by using cryptocurrencies, but the Fifth Circuit's ruling provides an early warning that at least in the near term courts are likely to be skeptical of claims that transacting in Bitcoin or other cryptocurrencies bestows Fourth Amendment protections on par with those afforded to CSLI in *Carpenter*. That position is likely to be tested, however, as cryptocurrency transactions become more common or pervasive, particularly if they can reach a point where they can paint a fairly comprehensive picture of a person's daily activities. Even then, however, "good faith" exceptions to the exclusionary rule might still leave criminal defendants without Fourth Amendment protection until privacy protections in such transactions are more firmly judicially recognized. It thus may be some time, if ever, before criminal defendants may be able to count on cryptocurrencies as a legally effective means to hide their activities from the government's detection.

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com