NORTON ROSE FULBRIGHT

Blockchain Law

Blockchain's Fourth and Fifth Amendment privacy paradoxes

New York Law Journal

January 28, 2025 | By **Robert A. Schwinger**

The author writes "Blockchain is frequently conceived of as a tool for confidentiality and privacy, but two federal court of appeals decisions from the latter part of last year highlight how limited that hope often proves to be, even in the face of federal constitutional protections."

Blockchain is frequently conceived of as a tool for confidentiality and privacy, but two federal court of appeals decisions from the latter part of last year highlight how limited that hope often proves to be, even in the face of federal constitutional protections.

In *Harper v. Werfel*, 118 F.4th 100 (1st Cir. 2024), decided this past September, and *Carman v. Yellen*, 112 F.4th 386 (6th Cir. 2024), decided several weeks earlier in August, two circuits wrestled with Fourth and Fifth Amendment challenges to government efforts to obtain individuals' blockchain transaction data.

The outcomes in these cases raise the question of whether these two constitutional provisions, despite being central to many privacy and confidentiality concerns, paradoxically may not have all that much to offer when it comes to realizing those goals in the blockchain world.

Getting caught in a "John Doe" summons from the IRS

In *Harper*, the plaintiff had made Bitcoin deposits into a digital currency exchange account but later liquidated those Bitcoin holdings or transferred them to a hardware wallet. Some time after, the IRS issued to that exchange a so-called "John Doe" summons for certain financial records pertaining to a wide range of customers including the plaintiff and their transaction histories.

A "John Doe" summons is "an ex parte third-party summons" that is issued "where the IRS does not know the identity of the taxpayer[s] under investigation," but only "following a court proceeding in which the IRS establishes that certain statutory criteria have been satisfied" and the summons is "narrowly tailored" to showing potential tax code noncompliance by individual taxpayers, per 26 U.S.C. § 7609(f).

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP. Gage Raju-Salicki, an associate in the firm's financial institutions disputes group, assisted in the preparation of this column.

The subpoena here sought customer transaction records from the exchange that would show taxpayer ID numbers, names, dates of birth, addresses, account activity records reflecting "the date, amount, and type of transaction (purchase/sale/exchange), the post transaction balance, and the names of counterparties to the transaction," and the customers' account statements.

The IRS obtained such information from the exchange in response to the subpoena, and the plaintiff subsequently received a notification from the IRS that he might not have properly reported certain of his virtual currency transactions.

The plaintiff responded by commencing an action alleging, inter alia, that the IRS's ex parte "John Doe" summons to the digital currency exchange violated his Fourth and Fifth Amendment rights. He sought relief requiring the IRS to return or destroy the records pertaining to his account that it had obtained from the exchange. His claims were dismissed by the district court, however, and the dismissal was affirmed by the First Circuit.

Fourth Amendment privacy rights

The First Circuit framed its Fourth Amendment analysis by noting that Fourth Amendment violations can consist either of "an intrusion upon a person's reasonable expectations of privacy," per *Katz v. United States*, 389 U.S. 347, 351 (1967), or a "physical intrusion on a constitutionally protected area," per *Carpenter v. United States*, 585 U.S. 296, 304 (2018). The plaintiff argued both, claiming that he had a reasonable expectation of privacy in his account information, and that his account records constituted his personal property. The First Circuit rejected each of these claims.

The court explained that the "reasonable-expectation-of-privacy" inquiry contains both subjective and objective elements. Not only must the plaintiff have an actual subjective expectation of privacy, but that expectation, "viewed objectively," also "must be justifiable under the circumstances" (quotations omitted). The court held that while the plaintiff may indeed have subjectively expected his account information to remain confidential, that expectation was not "justifiable" in these circumstances.

Citing *Smith v. Maryland*, 442 U.S. 725 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), the court explained:

> "The Supreme Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. This principle holds true even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. Of particular relevance here, the court held . . . that an individual has no legitimate expectation of privacy in information kept in bank records, as these documents, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." (Quotation and citations omitted.)

The court held that this principle — commonly referred to as the "third party doctrine" — applied to the account information the IRS had obtained through its subpoena:

> "All the information revealed to the IRS pursuant to the enforced summons -- personal identifiers such as taxpayer identification number, name, and address; records of account activity such as transaction logs; and statements -- is directly analogous to the bank records at issue in *Miller* -- checks, deposit slips, and financial statements."

The court also cited approvingly to the Fifth Circuit's similar conclusion in *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020) (discussed in R. Schwinger, "A little less privacy: Cryptocurrency transactions under the fourth amendment," N.Y.L.J. (July 27, 2020)). It also noted that the exchange's terms of service "expressly warn accountholders of the possibility of disclosure to law enforcement."

The plaintiff sought to counter these principles by citing to *Carpenter*, where the Supreme Court held that individuals have a reasonable expectation of privacy in the time-stamped records of their approximate location that are generated each time the individual's cell phone connects to the wireless network.

But this cellphone location information, the First Circuit explained, "has little in common" with the digital currency

exchange account records at issue in this case, because "the information contained in financial records like those at issue here, even several years' worth of them, does not paint nearly so detailed a portrait of an individual's daily activity" as the "detailed chronicle of a person's physical presence compiled every day, every moment, over several years," that was at issue in *Carpenter*. Rather, it said, whatever "intimate information" these records might reveal was little different from what is found in "traditional bank records."

Moreover, it noted, while carrying a cell phone may be "indispensable to participation in modern society," and the phone's location data is recorded "without any affirmative act on the part of the user beyond powering up," the same is not true of participating in digital currency transactions through an exchange. It noted that participating in a digital currency exchange is "not indispensable," and that transactions on such an exchange "occur only when a user opts into that activity."

Finally, the court rejected the plaintiff's contention that third-party doctrine cases like *Miller* are distinguishable on the theory that "'[c]ryptocurrency transactions are confidential by nature' thanks to the anonymity of the blockchain, a pseudonymized public ledger of all Bitcoin transactions." Notwithstanding that "exposure of a person's identity opens a potentially wide window into that person's financial activity contained on [the blockchain] ledger," the court concluded that the information here concerning financial transactions is, "fundamentally, much more analogous to the financial information at issue in *Miller* than to the uniquely comprehensive, locational data at issue in *Carpenter*."

The court went even further, questioning why "the decision to transmit financial information to the public -- even pseudonymously -- makes the expectation of privacy more reasonable than doing so privately" (emphasis in original). It noted that the plaintiff "could have bypassed a digital currency exchange" and instead "conducted his Bitcoin transactions through decentralized, peer-to-peer transactions," but chose to sacrifice that greater level of privacy for the technological convenience of using "an intermediary."

In so doing, said the court, he "voluntarily divulged information about his Bitcoin transactions" to the exchange, thus vitiating any reasonable expectation of privacy in his account information.

Lack of protectible property interests in account information

Plaintiff alternatively argued that he had a "property interest" in his account records that the IRS subpoena violated, but the court observed that he made no effort "to explain the legal source of the interest he asserts," instead only pointing vaguely to statements in Justice Gorsuch's dissenting opinion in *Carpenter* that cellphone customers may have property interests in their location data. See 585 U.S. at 405-06.

The court dismissed as "facile" the plaintiff's "simple" assertion that "that the property interest exists because these records are his 'papers,'" which is a word the Fourth Amendment uses to identify items it protects.

Moreover, the court noted that most of the records obtained through the summons were not the plaintiff's own "private papers" after all, but rather were documents generated by the exchange, such as records of transactions the exchange facilitated and periodic account statements, or were simply basic biographical information necessary to open an account. Thus, "we see no basis to conclude that the IRS intruded upon [plaintiff's] protected property rights."

The Fifth Amendment follows course

Plaintiff's claims under the Fifth Amendment fared no better. While he claimed that the IRS's ex parte summons deprived him of his "property rights" in his account records without notice or an opportunity to be heard, the court held that this claimed property interest was "no different from the one we rejected in connection with his Fourth Amendment claim."

Turning to an alternative prong of Fifth Amendment liability, the court agreed that there is a "substantive component of the Due Process Clause" that "protects a limited liberty interest in the confidentiality of certain intimate information."

However, even if the plaintiff were "correct that this protectable privacy interest may encompass certain sensitive financial information," that fact was of no avail in regard to information as to which the court already had concluded "he lacked any reasonable expectation of privacy in the circumstances here." The court thus rejected the plaintiff's Fifth Amendment claim as well. The First Circuit thus affirmed the dismissal of the plaintiff's complaint.

Mandatory reporting of crypto transactions

Fourth and Fifth Amendment claims in regard to disclosure of cryptocurrency transactions also featured in the Sixth Circuit's recent decision in *Carman v. Yellen*, but there the focus turned on to what extent, if at all, the plaintiffs even had standing to raise such claims and whether they were ripe and justiciable.

Carman involved the cash transactions reporting requirement for trade or business transactions over $10,000 under the Internal Revenue Code, 26 U.S.C. § 6050I(a), which requires for such transactions disclosure of the sender's name, address and taxpayer ID number, and the amount, date and nature of the transaction, as well as the recipient's own taxpayer ID number, name and address. However, the 2021 Infrastructure Investment and Jobs Act amended the definition of "cash" in this provision to include "any digital asset." Id. § 6050I(d)(3).

The *Carman* plaintiffs — who included persons who take payments in crypto, crypto miners who receive crypto as compensation for validating transactions, a crypto industry non-profit that receives contributions in crypto, and persons who make payments in crypto to advocacy and religious groups as part of their personal expressive activities — objected to this reporting requirement now being applied to digital assets.

They asserted various claims against this new requirement, including Fourth and Fifth Amendment challenges, as well as the claimed impact on their First Amendment rights and an enumerated-powers challenge to Congress's ability to even pass this law. Their constitutional claims were based in large measure on the fear that such reporting "will in turn lead to the government discovering transactions in which [they have] participated through public-ledger analysis; 'improper disclosure' of private information; and the 'uncover[ing]'" and chilling of their "'expressive associations,'" as well as time burdens and potential compliance costs with lawyers and accountants.

The defendants responded by challenging the plaintiffs' standing to raise these claims, and the justiciability and ripeness of such claims on a facial challenge to the statute. The district court agreed and dismissed the complaint. On appeal, the Sixth Circuit upheld the dismissal of the Fifth Amendment claims but staked out a limited area in which the plaintiffs might have standing to raise a ripe Fourth Amendment challenge, though without ruling on whether such a challenge would be substantively valid.

Unripe Fifth Amendment issues

The plaintiffs raised a Fifth Amendment due process vagueness argument against the new law, but the Sixth Circuit rejected this argument as improperly raising "hypothetical" issues about how the law "might apply" as to various kinds of transactions in which "plaintiffs may never engage."

The court noted that "[p]laintiffs ask us to evaluate the facial constitutionality of §6050I against transactions that may never occur and that plaintiffs themselves may never undertake," but "[w]e cannot invalidate §6050I based on scenarios that may never come to pass." While "it is possible that plaintiffs could be ultimately correct that certain provisions of §6050I could be vague, we do not have a constitutional license to issue an advisory opinion on these questions in the abstract" (emphasis in original).

The plaintiffs also challenged the reporting requirement as potentially raising Fifth Amendment self-incrimination claims. Here again, though, the court agreed such a claim was not ripe "until a claim of the privilege is actually made" in response to the reporting requirement.

Nuanced path for Fourth Amendment claims

The *Carman* plaintiffs also raised Fourth Amendment claims. Those claims were based largely on the premise that "the government will undertake substantial investigative efforts to connect the transactions they must report to the public ledger, then to discern what the plaintiffs' addresses are, and then to discover a litany of undisclosed transactions that may offer insight into the intimate details of plaintiffs' lives," thereby invading their Fourth Amendment rights. The court held this suggestion too "abstract" and speculative to be ripe, however.

Nevertheless, the court did find ripe one limited aspect of the plaintiffs' Fourth Amendment claim — that the mere disclosure of required information to the government, irrespective of what use the government might make of that information, violated the plaintiff's Fourth Amendment rights. The court held that this claim was ripe to be adjudicated because it did not involve any "speculative scenarios" and required "no further factual development."

The court also held that plaintiffs had standing to raise such a claim. "Plaintiffs have pleaded that they will engage in at least some transactions that require § 6050I reports" (emphasis in original). Thus, "there is no question that, per the amended complaint's allegations, at least some of the plaintiffs will have to report at least some of their transactions."

Having alleged that "the very disclosure of the information required by §6050I is injurious, and because plaintiffs have pleaded they will have to make the disclosures, they have suffered an injury in fact as the direct objects of the action at issue." Whether or not this claim might fail on the merits had no bearing on whether the plaintiffs had standing to assert it, and the court noted it was required to accept the allegations upon which the claim rested at this stage.

Thus, without addressing their merits, the Sixth Circuit held a limited portion of the plaintiffs' Fourth Amendment claim was sufficiently justiciable to be able to proceed, reversing the district court on this point. The court likewise upheld ripeness and standing as to plaintiffs' enumerated-powers and First Amendment claims on grounds similar to those applicable to their Fourth Amendment claims.

Conclusion

While blockchain users may aspire to have the technology cloak their transactions in privacy and confidentiality from the government and outside parties, the extent to which the law enables them to realize that goal may sometimes fall short of their hopes. Despite the constitutional protections of the Fourth and Fifth Amendments that are designed in many respects to help protect privacy and avoid forced disclosure of information, *Harper* and *Carman* illustrate that these constitutional provisions may offer only limited protection (if that) to make such goals a reality.

These cases also highlight how the decision whether to hold and transact in digital assets through an exchange, versus self-custodying the assets and engaging in decentralized peer-to-peer transactions, is not merely a matter of personal convenience. Rather, it may in fact have a substantial impact on whether blockchain users can achieve the privacy and confidentiality they may desire.

Although self-custodying does not exempt users from having to comply with reporting requirements like §6050I, it may limit the government's ability to obtain such information through alternative avenues like a "John Doe" summons to third parties. Self-custodying may also prove particularly important if privacy or anonymity is sought to facilitate potentially sensitive expressive activity, such as political, religious or ideological contributions or support.

In short, heaven may help those blockchain users who help themselves, because the Fourth and Fifth Amendments may fall somewhat short in giving them the full extent of the protections they might desire.

The public-facing nature of blockchain ledgers and the widespread use of intermediaries like exchanges can pose significant obstacles to achieving the privacy, confidentiality and anonymity that many users may hope to achieve through blockchain transactions. At present, it does not seem that looking to the Fourth and Fifth Amendments will reliably provide a path to mitigating those concerns.

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 3000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

nortonrosefulbright.com