INSTITUTE FOR JUSTICE

March 29, 2021

VIA ELECTRONIC SUBMISSION

Kenneth A. Blanco
Director, Financial Crimes Enforcement Network
FinCEN Policy Division
P.O. Box 39
Vienna, VA 22183

Re: FinCEN-2020-0020, RIN 1506-AB47, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

Dear Director Blanco:

The Institute for Justice ("IJ") is a national public interest law firm dedicated to securing Americans' constitutional rights. In that capacity, IJ has significant experience representing individuals accused of violations of the anti-structuring provisions of the Bank Secrecy Act regime. IJ also has significant experience challenging government laws and regulations under the U.S. Constitution, including under the Fourth Amendment. And IJ is also affected by the Proposed Rule in more practical respects, as well, as IJ accepts donations from individuals in the form of cryptocurrency and has an interest in maintaining the privacy of its donors. IJ submits this comment letter because IJ is concerned that the Proposed Rule, if adopted, would enact an intrusive and unnecessary government surveillance program in violation of the Fourth Amendment and other provisions of the U.S. Constitution.

INTRODUCTION

The Proposed Rule would open up transactions involving cryptocurrency to an unprecedented degree of governmental scrutiny. The Proposed Rule imposes recordkeeping and reporting obligations for cryptocurrency transactions over $10,000 (and, in some respects, even for transactions over $3,000), including an obligation for financial institutions to record and report the identities and addresses of counterparties to transactions initiated by the institution's customers. Because of the nature of cryptocurrency, the recording and reporting of that kind of identifying information has significant privacy implications: For Bitcoin and other similar cryptocurrencies, all transactions associated with a particular wallet ID are recorded indelibly on the public blockchain, meaning that, once the government associates a wallet ID with a specific individual, the government can identify *every other past and future transaction* conducted by that individual using that wallet ID. And, thanks to sophisticated analytic tools, the government can often link that individual with additional wallet IDs as well. Under the Proposed Rule, the government would collect all of this sensitive data without any showing of individualized suspicion at all.

901 N. Glebe Road, Suite 900 Arlington, VA 22203 (703) 682-9320 (703) 682-9321 Fax
general@ij.org www.ij.org

The resulting surveillance dragnet would sweep up significant information as a result of completely ordinary and legitimate transactions. A Bitcoin user might spend over $10,000 to purchase an automobile,[1] furniture,[2] or even a house.[3] Or a Bitcoin user might donate over $10,000 to a nonprofit organization like the Institute for Justice.[4] Then, as a result of that one single transaction, the financial institution associated with the seller (or the nonprofit organization) would be compelled to determine and then report the Bitcoin user's identity to the government. And the government could then link that Bitcoin user to every transaction ever conducted by that individual with that wallet ID—including purchases of medical tests or sexually-explicit materials,[5] gifts to artists,[6] or donations to other non-profit organizations[7]—whether over $10,000 or not. And if the Bitcoin user attempted to structure his affairs to minimize that disclosure, he would risk prosecution under the structuring laws.

That proposed surveillance program raises a number of serious constitutional concerns. First, the Proposed Rule raises precisely the kinds of concerns that led the Supreme Court to find a violation of the Fourth Amendment in *Carpenter v. United States*;[8] just as the cell-site locational data at issue in that case included vast amounts of information concerning individuals' whereabouts, the reporting mandated by the Proposed Rule would allow financial institutions to unlock vast amounts of sensitive financial data. Second, the Proposed Rule also raises serious concerns under the Fifth Amendment's privilege against self-incrimination, as it forces users of cryptocurrency to disclose identifying information that they might otherwise keep private—and orders such disclosure for no purpose beyond detecting crime. Third, that compelled disclosure constitutes compelled speech and raises significant First Amendment concerns; and those concerns are amplified further when the compelled speech forces nonprofit organizations to identify their donors. And, finally, the Proposed Rule also raises serious due process concerns insofar as it conscripts financial institutions into the role of law enforcement.

Meanwhile, the entire Bank Secrecy Act regime has morphed in ways that have greatly expanded its reach as compared to the regime upheld by the Supreme Court in *Shultz* and *Miller*.[9] Whereas the Supreme Court in those cases observed that banks were simply being required to keep records and file limited discrete reports, financial institutions today are forced to essentially serve a law enforcement function vis-à-vis their own customers. The volume of reporting has significantly increased over the years. And, today, it is even illegal for customers to

---

[1] Sam Shead, *Elon Musk says people can now buy Tesla with bitcoin*, CNBC (Mar. 24, 2021), https://cnb.cx/3ckmGYa.

[2] Jacob Bernstein, *What Can You Actually Buy With Bitcoin*, N.Y. Times (Feb. 3, 2021), https://nyti.ms/3rlxolv.

[3] Kathleen Elkins, *Here's the one thing you need to buy a house with bitcoin*, CNBC (Jan. 3, 2018), https://cnb.cx/3d5OheO.

[4] Institute for Justice, *IJ Receives Pineapple Fund Grant*, Liberty & Law (Apr. 2018), https://bit.ly/31cRAvn.

[5] Bernstein, *supra*, note 2.

[6] Sarah Cascone, *A French Street Artist made $1,000 After Adding a Bitcoin QR Code to His Murals*, ArtNews (May 14, 2018), https://bit.ly/3f8o5TD.

[7] Andrea Tinianow, *Bitcoin Donations Poised To Transform Nonprofits*, Forbes (Nov. 21, 2019), https://bit.ly/3vWsZZP.

[8] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[9] *California Bankers Association v. Shultz*, 416 U.S. 21 (1974); *United States v. Miller*, 425 U.S. 435 (1976).

structure their affairs to avoid this reporting regime. Today's sweeping surveillance system should be carefully reevaluated—not expanded further to new technologies.

Finally, even as the scope of bank reporting has been expanding, the doctrinal foundations for that surveillance program have been eroding. Several members of the Supreme Court have expressed support for a property-rights based view of the Fourth Amendment, under which privacy would be determined by property and contract. Under that approach, individuals should be able to secure the privacy of their banking information through private contracts. At the same time, as *Carpenter* demonstrates, Justices applying the traditional reasonable expectation of privacy approach have also recognized that the third-party doctrine is incompatible with our modern society—where individuals necessarily share significant private data with a broad array of third parties. The eroding doctrinal underpinnings of the Bank Secrecy Act regime caution strongly against expanding that regime to an entirely new context.

DISCUSSION

1. Extension Of The Bank Secrecy Act To Cryptocurrency Would Raise Serious Constitutional Concerns.

The Proposed Rule raises privacy implications that are entirely different in kind from those raised by the original Bank Secrecy Act upheld by the Supreme Court in *Shultz* and *Miller*. When a bank reports an over-$10,000 cash transaction, the government receives just a single piece of information: that a particular customer withdrew or deposited $10,000 or more in cash. The customer's use of those funds remains a private matter. By contrast, the records and reports required by the Proposed Rule provide the government with a key to interpret the public blockchain, opening a window onto both the downstream use of the funds after the reported transaction and other unrelated transactions (both in the past and the future) on the blockchain. Far from conveying a single discrete piece of information, such a report allows the government to engage in extensive surveillance of completely unrelated financial transactions. That intrusive surveillance raises serious concerns under at least four separate constitutional provisions.

a. Fourth Amendment

First, the Proposed Rule would raise precisely the concerns that led the Supreme Court to find a Fourth Amendment violation in *Carpenter*. In *Carpenter*, the Court explained that government access to locational data generated by cellphones could not be justified under the third-party doctrine—the same doctrine originally developed to uphold the Bank Secrecy Act—because the doctrine did not adequately account for the "seismic shifts in digital technology that make possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." Just as the cell-site data at issue in *Carpenter* would provide "a detailed chronicle of a person's physical presence," the data required by the Proposed Rule would provide the government with the means to compile a "detailed chronicle" of every financial transaction—past or present—conducted with a wallet ID.

Indeed, Justice Kennedy's *Carpenter* dissent points to precisely these concerns. Justice Kennedy, joined by Justices Thomas and Alito, observed that the "troves of intimate information the Government can and does obtain using financial records . . . dwarfs what can be gathered from cell-site records," including "a comprehensive account of almost every transaction an individual makes on a daily basis." These concerns are ameliorated somewhat in the context of ordinary currency reporting, given the discrete and limited nature of the information that is required to be reported to the government—though, as explained below, these concerns are legitimate even there. But these concerns assume even greater significance in the context of the far greater disclosure required by the Proposed Rule. The complete financial picture available on the blockchain differs qualitatively from the singular financial transaction at issue in ordinary currency reporting. A single $10,000 transaction (say, purchasing an automobile) would allow the government to associate an individual with every other transaction ever conducted with a wallet ID.

The scope of this intrusion is exacerbated further by other aspects of the Proposed Rule. The Proposed Rule would require not just that financial institutions share information about their customers' counterparties, but that they collect and verify the accuracy of that information as well. Drafting financial institutions and ordering them to create, verify, and maintain records so the government can search them later commandeers those financial institutions as the government's agents.[10] By conscripting financial institutions to gather information that would not otherwise exist, the Proposed Rule allows the government to obtain information that might otherwise be unavailable even with a warrant. Moreover, given the ubiquity of hosted wallets, there is no practical way for a customer who wants to use cryptocurrency to avoid being subject to the Proposed Rule. Bitcoin and other electronic currencies have an increasingly large role in modern life, and the number of uses for blockchain technology has only grown in recent years. But if the Proposed Rule were enacted, customers would be put to the choice of participating in the modern electronic currency economy or retaining the full measure of their Fourth Amendment rights.

While the Supreme Court upheld the Bank Secrecy Act against a Fourth Amendment challenge in *Shultz*, its reasoning cannot be extended to the new and different context presented by the Proposed Rule. The Court there noted that the Act only required "reporting of information with respect to abnormally large transactions in currency, much of which information the bank as a party to the transaction already possesses or would acquire in its own interest." This narrow reporting was "sufficiently described and limited in nature, and sufficiently related to a tenable congressional determination as to improper use . . . so as to withstand the Fourth Amendment challenge." By contrast, the information required here is not information that a financial institution would normally possess, as there is no reason why a financial information would ordinarily need to identify the counterparties to a customer's cryptocurrency transactions. And

---

[10] *See, e.g.*, *Skinner v. Ry. Lab. Executives' Ass'n*, 489 U.S. 602 (1989) (holding that regulations authorizing railroads to perform warrantless drug tests of engineers involved in accidents implicated the Fourth Amendment).

the information is by no means limited in scope. The discrete reporting upheld in *Shultz* bears no resemblance to the far more sweeping intrusion contemplated by the Proposed Rule.

b. Fifth Amendment

The Proposed Rule also raises significant concerns under the Fifth Amendment's protections against self-incrimination.[11] The rule would compel owners of both hosted and unhosted wallets to provide the government with identifying information that, because of the nature of the public blockchain, offers the key to interpret their past and future financial history. The government's express purpose in collecting that information is to scour the blockchain for incriminating information. As such, the Proposed Rule forces cryptocurrency users to serve as their own informants. That blanket requirement of self-incrimination cannot be reconciled with a proper understanding of the Fifth Amendment.

The Firth Amendment concerns here are vividly illustrated by *Marchetti v. United States*, which held that the Fifth Amendment privilege against self-incrimination barred a conviction for failure to file a tax report concerning gambling activities that were illegal under state law.[12] The Court explained that "[s]ubstantial hazards of incrimination as to past or present acts plainly may stem from the requirement to register" because registration "increases the likelihood that any past or present gambling offenses will be discovered." Here, those "substantial hazards" are even greater, as the entire purpose of the Proposed Rule is to search for potential crimes. To be sure, not every person subject to the Proposed Rule is engaged in criminal activity. But an individual need not demonstrate that she is guilty of a crime in order to invoke the Fifth Amendment. Indeed, limiting the Fifth Amendment to confessed criminals would be entirely circular, as an individual would need to give up her Fifth Amendment rights in the process of invoking them. Whether a person is guilty of an offense or not, the government cannot force her to act as her own informant.

The Supreme Court's opinion in *Shultz* upheld the original Bank Secrecy Act against a Fifth Amendment challenge, but its reasoning cannot be extended to the Proposed Rule. The Court in *Shultz* explained that banks already had access to all the information that they were required to record and report, as "banks voluntarily kept records of this sort before they were required to do so by regulation." And customers could not raise a Fifth Amendment challenge to any further disclosure of that information by the banks, as "a party incriminated by evidence produced by a third party sustains no incrimination of his own Fifth Amendment rights." By contrast, the Proposed Rule would force financial institutions to demand information from their customers that they would ordinarily have no reason to request, and would then force financial

---

[11] *See Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting) ("[T]here is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence."); *see also Boyd v. United States*, 116 U.S. 616, 631–32 (1886) ("[E]xtorting the party's oath, or compelling the production of his private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government.").

[12] *Marchetti v. United States*, 390 U.S. 39 (1968).

institutions to disclose that information to the government. The Fifth Amendment bars law enforcement from requiring that kind of compelled self-incrimination.

c. First Amendment

The disclosure of information required by the Proposed Rule also raises significant concerns under the First Amendment. As applied to nonprofit organizations that accept donations of cryptocurrency—including the Institute for Justice—the Proposed Rule would significantly burden the associational rights of both organizations and their donors. If a donor were to contribute over $10,000 to an organization's hosted wallet, the financial institution hosting the wallet would be required to disclose not just the donation but also the donor's name and physical address, thereby allowing the government to scour the donor's past and future cryptocurrency use. Or, if a donor used $10,000 to purchase an automobile, house, or other consumer good, the resulting disclosure would likewise reveal all the donor's under-$10,000 donations as well. That kind of intrusion cannot be squared with the First Amendment, as "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association."[13]

The ACLU raised similar concerns in *Shultz*, but the Supreme Court rejected the claim on the ground that the ACLU had not actually explained how the Bank Secrecy Act would "require the reporting of information with respect to the organization's financial activities." The same cannot be said here. Increasingly, nonprofit organizations accept donations in the form of cryptocurrency, and it is hardly unheard of for nonprofits to accept donations over $10,000. The Institute for Justice, for instance, has previously received donations of over $10,000 in cryptocurrency in its hosted wallet. And while a nonprofit could deposit a $10,000 cash donation in the bank without disclosing the identity of its donor, a nonprofit with a hosted wallet could not accept an over $10,000 donation of cryptocurrency without opening a window for the government to canvass the donor's entire history on the blockchain.

Moreover, these First Amendment concerns are not limited to nonprofit organizations and their donors. Other individuals and organizations also have associational First Amendment rights. And the compelled disclosure discussed above in the context of the Fifth Amendment also involves compelled speech: The Supreme Court has held that the type of data generated by the Proposed Rule constitutes speech, and the Proposed Rule forces parties and counterparties to cryptocurrency transactions to generate such speech on a massive scale.[14]

---

[13] *NAACP v. Patterson*, 357 U.S. 449, 462 (1958); *see also Shelton v. Tucker*, 364 U.S. 479 (1960); *Bates v. City of Little Rock*, 361 U.S. 516 (1960).

[14] *See Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011); *United States v. United Foods, Inc.*, 533 U.S. 405, 410 (2001).

d. Due Process

Finally, the Proposed Rule also raises significant due process concerns, insofar as it forces financial institutions to assume a role as an agent of law enforcement. The plaintiffs in *Shultz* raised this concern about the original Bank Secrecy Act, arguing that it violated due process insofar as it would "make the banks the agents of the Government in the surveillance of its citizens." But the Supreme Court held that the banks were "not conscripted neutrals," and, to the contrary, "Congress not illogically decided that if records of transactions of negotiable instruments were to be kept and maintained . . . the bank was the most easily identifiable party to the instrument and therefore should do the recordkeeping." In other words, the Bank Secrecy Act simply required banks to retain records of information that was already in their possession. The Proposed Rule, by contrast, requires financial institutions to actively solicit information that they would not normally possess as part of a transaction, which they are then required to make available to law enforcement; a bank hosting a nonprofit, for instance, would need to demand and report the identity of the organization's donors, and a bank hosting a for-profit business would likewise need to demand and report the identities of its customer's customers. The Proposed Rule violates due process insofar as it conscripts financial institutions and compels them to police their own customers.

2. The Bank Secrecy Act Is Fundamentally Broken And Has Come Unmoored From The Rationale Of *Shultz* and *Miller*.

At the same time as the Proposed Rule extends the Bank Secrecy Act's regime into a new technological context, the Bank Secrecy Act's regime has also expanded and morphed in ways that have increasingly strayed from the rationale of *Shultz* and *Miller*. Those early cases conceived of the Bank Secrecy Act as simply requiring banks to maintain ordinary business records, while also reporting a handful of discrete financial transactions. Those decisions did not envision the surveillance juggernaut the Bank Secrecy Act regime has become today.

First, financial institutions today are required to analyze financial transactions in order to generate so-called "suspicious activity reports," or "SARs," which are intended to identify and alert law enforcement of suspicious activities engaged in by the bank's own customers. This is completely contrary to the reasoning of *Shultz*, which rejected any suggestion that the government could "make the banks the agents of the Government in surveillance of its citizens." These changes to the Bank Secrecy Act regime have changed it from a set of recordkeeping requirements and discrete reporting provisions into a vast surveillance dragnet that enlists banks and other financial institutions as *de facto* law enforcement agencies.

Second, *Shultz* and *Miller* could not possibly have foreseen the vast expansion of the volume of reports filed under the Bank Secrecy Act regime. For instance, in 2017 the president

of The Clearing House Association testified before Congress that "the largest banks file one SAR per minute."[15] He explained:

> Now that we have almost 2 million filed per year, there is no one reading them in the first instance. Instead, what law enforcement does is word searches against that database. The banks also do searches against the database, basically looking for patterns. So we have gone from sort of providing leads in a very personal way to a prosecutor to basically having a big bunch of data . . . .

A subset of those reports leaked to the public in 2020, and, although the reports constituted only about .02% of SARs filed between 2011 and 2017, they described over $2 trillion in transactions.[16] Far from the "sufficiently described and limited in nature" reporting envisioned by the Supreme Court in *Shultz*, financial institutions today are compelled to report vast amounts of information to the government without any judicial process or individualized showing of suspicion from law enforcement.

Finally, government has also tightened the grip of this surveillance regime by making it a crime to evade its grasp. Under structuring laws, individuals can be charged with a felony if they arrange their financial affairs in order to avoid triggering these various reporting requirements. These laws have ensnared innocent individuals who—for reasons of privacy—do not wish to have their financial transactions reported to the government, and they have also ensnared individuals who were "conducting legal activities and could provide a legitimate reason for the pattern of transactions" that resulted in the non-filing of a currency report.[17] For example:

- Carole Hinders, the proprietor of Mrs. Lady's Mexican Food, a small-town restaurant in Spirit Lake, Iowa, had more than $32,000 seized by the IRS after her mother told her that depositing more than $10,000 created a hassle for the bank.[18]

- Jeffrey, Richard, and Mitchell Hirsch, the proprietors of Bi-County Distributors, Inc., had over $446,000 seized by the IRS after they were advised by their accountant to

---

[15] Statement of Greg Baer, President, The Clearinghouse Association, *Examining the BSA/AML Regulatory Compliance Regime*, Hearing Before the Subcommittee on Financial Institutions and Consumer Credit: House Committee on Financial Services (June 28, 2017), https://www.hsdl.org/?view&did=818402.

[16] Madison Flowers, *Lessons from the FinCEN Files: A Call To Reform the Regulation of Money Laundering,* American Criminal Law Review (2020), https://www.law.georgetown.edu/american-criminal-law-review/wp-content/uploads/sites/15/2021/01/58-1-Flowers-Lessons-from-the-FinCEN-Files.pdf.

[17] *See* Treasury Inspector General for Tax Administration, *Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Small Businesses*, at 17 (Mar. 30, 2017), https://www.treasury.gov/tigta/auditreports/2017reports/201730025fr.pdf.

[18] *See United States v. Thirty-Two Thousand Eight Hundred Twenty Dollars and Fifty-Six Cents in U.S. Currency*, No. 13-CV-4102 (N.D. Iowa); *see also* Shaila Dewan, *Law Lets I.R.S. Seize Accounts on Suspicion, No Crime Required*, N.Y. Times (Oct. 25, 2014), https://nyti.ms/3eXfbIn.

keep cash deposits under $10,000 to reduce paperwork burdens for their banks, as banks often close the accounts of customers that make frequent large cash deposits.[19]

- Lyndon McLellan, the proprietor of a rural North Carolina convenience store, had more than $107,000 seized by the IRS after a bank teller told his niece (who typically made the deposits for the business) that depositing less than $10,000 would avoid unnecessary paperwork burdens.[20]

- David and Larry Vocatura, the proprietors of a third-generation family bakery, had $68,000 seized after a bank employee called the bakery to complain that over-$10,000 cash deposit required the bank to complete additional paperwork.[21]

Under the structuring laws, opting out of the government's surveillance program is no longer an option, and even individuals who are unaware of the government's surveillance program have been penalized for slipping its grasp.[22]

The expansion of the Bank Secrecy Act regime beyond its origins is significant, as it is far from clear that the Court in *Shultz* would have upheld the regime in its current form. Justices Powell and Blackmun, whose votes were necessary to form a majority, entered a concurrence stating that "[a] significant extension of the regulations' reporting requirements . . . would pose substantial and difficult constitutional questions."[23] That "significant extension" has in many ways already arrived. And the Proposed Rule would extend the regime an additional step further, by requiring disclosure of significant identifying information that would allow the government to essentially unlock the information on the blockchain.

The concerns raised by this expanding surveillance dragnet are no small matter. Financial privacy is an essential part of a free society: As Justice Powell observed in *Shultz*, "[f]inancial transactions can reveal much about a person's activities, associations, and beliefs." On some level, practically anything that anyone might want to do in life requires expenditures of money and, by following the flow of that money, government can obtain insight into almost the full sphere of activity throughout the nation. Today, the vast and expanding collection of data by the nation's financial institutions, as well as new technological developments including the public blockchain, are colliding with existing laws, regulations, and judicial doctrines in a way that is

---

[19] *See In the Matter of the Seizure of Four Hundred Forty Six Thousand Six Hundred Fifty One Dollars an Eleven Cents in U.S. Currency*, No. 14-mc-1288 (E.D.N.Y.); *see also* Dewan, *supra* n. 18.

[20] *See United States v. $107,702.66 in United States Currency*, No. 14-cv-00295 (E.D.N.C.); *see also* Shaila Dewan, *Rules Change on I.R.S. Seizures, Too Late for Some*, N.Y. Times (Apr. 30, 2015), https://nyti.ms/3c0xYAw.

[21] *See Vocatura's Bakery, Inc. v. Internal Revenue Service*, No. 16-mc-00147 (D. Conn.); *see also* Ryan Blessing, *Vocatura's to get seized money back; investigation continues*, Norwich Daily Bulletin (May 26, 2016), https://bit.ly/2P0qtRf; Ryan Blessing, *IRS withdraws grand jury subpoena against Norwich bakery*, Norwich Daily Bulletin (June 9, 2016), https://bit.ly/3s1XcEi.

[22] Congress has amended the law to institute some protections against property seizures in these situations, but those reforms do not apply to the law's criminal structuring prohibitions. *See* Taxpayer First Act, Pub. L. No. 116-25 § 1201 (July 1, 2019) (amending 31 U.S.C. § 5317(c)(2)).

[23] *Shultz*, 416 U.S. at 1525-26 (Powell, J., concurring).

astronomically increasing the government's ability to harness this type of data. Government should be considering whether there are ways to limit that vast and expanding surveillance architecture, in order to better preserve the essential values of a free society—not rushing to extend it into a new and different technological context.

3. The Categorical Third-Party Doctrine, As Exemplified By The Holdings In *Smith* And *Miller,* Rests On An Increasingly Vulnerable Doctrinal Foundation.

The expansion of the Bank Secrecy Act contemplated by the Proposed Rule should also be approached with hesitation because many of the decisions upholding the constitutionality of modern bank reporting laws rest on shaky ground. Recent advances in Fourth Amendment jurisprudence have demonstrated a renewed focus on both on a robust view of property rights and a concomitant refusal to accept that all information people share with others loses all constitutional protection.

The Supreme Court's renewed interest in a Fourth Amendment that turns on notions of property, rather than privacy, places doctrinal stress on the third-party doctrine. In *United States v. Jones*, the Supreme Court held the physical attachment of a tracking device onto someone's vehicle was a search that generally required a warrant.[24] It is a search because the Fourth Amendment protects one's property rights as established by the positive law, and violation of those rights constitutes a trespass actionable at common law.

But property rights do not exist only through deeds and bills of sale; property can also arise out of contracts between two consenting parties. For instance, a contract may provide that a mechanic act as a bailee towards a vehicle he or she is repairing. In that instance, the mechanic can fully stand in the shoes of the vehicle's owner, as numerous courts have recognized that a bailee has "a sufficient interest in bailed property to give them standing to object to its seizure or search."[25]

There is no reason those contractual rights need to flow only one way. A contract can just as easily give a customer the right to use a company's property, thereby placing that customer in the same position as the company itself. The majority in *Olmstead v. United States*, held that the wiretapping of the telephone lines outside Olmstead's home worked no Fourth Amendment injury, as Olmstead himself did not own those lines.[26] But in a prescient dissent, Justice Butler noted:

> The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission the exclusive use of

---

[24] *United States v. Jones*, 565 U.S. 400 (2012).

[25] *See, e.g., United States v. Perea*, 986 F.2d 633, 640 (2d Cir. 1993); *United States v. Benitez-Arreguin*, 973 F.2d 823, 829 (10th Cir. 1992) (holding that search of bag held by bailee was unconstitutional).

[26] *Olmstead v. United States*, 277 U.S. 438 (1928).

> the wire belongs to the persons served by it. Wire tapping involves interference with the wire while being used.

In other words, the telephone lines that Olmstead used were his lines from a property rights perspective. He and the telephone company entered into a contract whereby Olmstead agreed to pay money in exchange for use of the telephone company's facilities. According to Justice Butler, Olmstead had just as much right to complain about the wiretapping as he would if a government agent had secreted himself in a hotel room Olmstead had rented.

This positive law conception of property should apply with equal force no matter whether the item shared via contract is physical or informational. When a customer initiates a relationship with a bank, they agree by contract that the customer will provide the bank with certain information. The bank would then use that information to perform financial services on the client's behalf. In other words, just as with the mechanic example above, the parties voluntarily agreed that the bank would take and hold onto this information for a specified contractual end. Although the mechanic could violate that contract, say by driving the car to the police station for an inspection, the mere fact he *could* do so does not mean the police can break into every vehicle at the mechanic's shop. For the same reason, it makes no sense to hold that because the bank *could* violate its contract by voluntarily divulging its depositor's records to the police, those same police now have warrantless access to every record in the bank's possession.

This simple comparison shows how the third-party doctrine as currently conceived violates a property-rights/positive law theory of the Fourth Amendment. Our property is not merely a pile of physical things. Indeed, the Fourth Amendment specifically enumerates papers as a category of protected property precisely because of the non-physical thoughts and feelings those papers contained. The fact those same thoughts and feelings now rest on third-party servers pursuant to contract should make no difference. After all, contracts are how we convey one or more of the "sticks" associated with property. If customers and firms agree to secure the customer's data from unwarranted government search, that is a decision the positive law (and the Constitution) should respect. And giving full respect to that private ordering means treating the customer's data with full Fourth Amendment protection, including the requirement that a judge issue a warrant prior to its compelled disclosure.

Moreover, the Court's recent property-rights resurgence is not the only threat to the third-party doctrine's continued vitality. In her *Jones* concurrence, Justice Sotomayor wrote about how, in the future, government agents could get Jones' location information not from installing a GPS tracking device, but by instead subpoenaing that same information from companies with whom Jones shared that data. Recognizing the long-term threat such technological advances pose, Justice Sotomayor stated that "[m]ore 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."[27] Viewing the third-party doctrine enabled by *Miller* as "ill suited to the digital age, in which people reveal a great deal of information about themselves to third

[27] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

parties in the course of carrying out mundane tasks," Justice Sotomayor refused to "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."

The Court soon put Justice Sotomayor's concurrence to the test in *Carpenter*. The facts in *Carpenter* echo Justice Sotomayor's fact pattern: Carpenter had contracted with his cell phone company for service, and, to get that service, Carpenter's phone had to ping cell phone towers. The record of those pings, known as cell site location information (CSLI), provided a rough map as to Carpenter's travels, a map that would only grow in precision as technology progressed. As noted above, the Court found that the resulting "exhaustive chronicle of location information" could not be casually disclosed under the third party doctrine. And the Court also observed that the generation of such data was difficult to escape in the modern world: A cell phone begins automatically pinging cell towers whenever it is in operation, and this action is necessary in order for the phone to work at all. In such a circumstance, said the Court, "in no meaningful sense does the user voluntarily 'assume[ ] the risk'" that their information will be shared with the government.

Thus, *Carpenter* shows that to the extent the third-party doctrine has continued viability under the reasonable expectation of privacy framework, that viability exists only when a person voluntarily shares discrete data that reveals little in the way of "identifying information." And, as explained at greater length above, none of that can be said for the Proposed Rule.

Citizens should not be forced to sacrifice their constitutional rights in order to participate in modern society. Yet that is precisely what the Proposed Rule would require. Because requiring banks to collect, store, and transmit personally identifying information associated with uncovered wallet IDs impinges on customers' rights under the positive law and their reasonable expectations of privacy, it constitutes a search for which the government should be required to secure a warrant. Because the Proposed Rule in no way requires a warrant or similar judicial authorization, it should be rescinded.

Sincerely,

Robert Frommer
Senior Attorney
Institute for Justice

Robert E. Johnson
Senior Attorney
Institute for Justice