TESTIMONY OF

Peter Van Valkenburgh

Research Director of Coin Center[1]

BEFORE THE

Subcommittee on Digital Assets, Financial Technology and Inclusion

Decoding DeFi: Breaking Down the Future of Decentralized Finance

September 10, 2024

In the late 1940s, there were 350,000 telephone switchboard operators in the U.S.[2] Privacy-conscious Americans worried that operators might still be listening to their calls after connection, and that concern wasn't unfounded. In the 1928 Supreme Court decision *Olmstead v. U.S.*, wiretapping was deemed not to violate the Fourth Amendment.[3] This allowed police to listen to conversations without proof of reasonable suspicion, or judicial oversight, and use that evidence in court.

By the end of the 20th century, two significant changes occurred. In 1967, the Court overturned *Olmstead* in the landmark decision *Katz v. U.S.*[4] By the 1980s, computers and automation had

[1] Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies.We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

[2] Tim Taylor, *Telephone Operators: The Elimination of a Job*, Conversable Economist (June 21, 2021), https://conversableeconomist.com/2021/06/21/telephone-operators-the-elimination-of-a-job/.

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

[4] *Katz v. United States*, 389 U.S. 347 (1967).

largely replaced telephone operators, and by the 90s, strong end-to-end encryption ensured communication intermediaries were blind to message contents.[5]

Today, there are around 600,000 licensed stock brokers in the U.S.[6]—fewer brokers per person than telephone operators in the 1940s. Like the operators of the past, financial intermediaries can and do learn intimate details of your life. However, in the 1976 decision *Miller v. U.S.*, the Supreme Court ruled that Americans have no reasonable expectation of privacy in their financial records.[7]

Fortunately, in the 21st century, two things are changing once again. First, many financial transactions no longer require a human intermediary—a concept known as DeFi.[8] Second, the Court is poised to overrule *Miller* and vindicate privacy rights, just as they did with *Olmstead*.[9]

---

[5] End-to-end encryption is most visibly discussed in the context of messaging systems such as Signal Encrypted Messaging, WhatsApp, or Apple Messages, these systems reliably blind all third parties to the contents for the messages. This is not, however, a niche or exceptional development in communications. Almost all web activity today is transmitted over the Transport Layer Security (TLS) protocol (visible when you visit a website via an https: rather than http: prefix). Communication intermediaries like Verizon or Comcast cannot decode the data being exchanged between you and the host of the website you are visiting. In this way, the communications intermediary has become incapable of listening in on your activities. Many people do much of their day to day activities on major web platforms, like Meta's Facebook or Google's Workplace services and these activities can be surveilled by the maintainers of those websites but the data is still shielded from communications intermediaries and still end-to-end encrypted in the sense that the user is one end and the platform maintainer is the other end.

[6] FINRA, *Statistics*, FINRA.org, https://www.finra.org/media-center/statistics (last visited Aug. 22, 2024).

[7] United States v. Miller, 425 U.S. 435 (1976) (Holding that individuals do not have a reasonable expectation of privacy in their financial records held by a third party, such as a bank. This decision established what is now known as the third-party doctrine exception to the warrant requirement for search and seizure.).

[8] Landon Zinda, *How Congress Should and Should Not Approach DeFi*, Coin Center (Mar. 2, 2023), https://www.coincenter.org/how-congress-should-and-should-not-approach-defi/.

[9] See Peter Van Valkenburgh, *Electronic Cash, Decentralized Exchange, and the Constitution*, Coin Center (Nov. 2019), https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/ ("Recently, the third-party doctrine has come under attack from justices and legal scholars who believe it is predicated on an outmoded understanding of the modern information landscape and who fear that it is today used to enable truly massive private data collection with little to no judicial process or accountability.86 As people increasingly hand the entirety of their private correspondence and data over to cloud service providers and other online intermediaries, there grows, effectively, a gaping hole in our once comprehensive Fourth Amendment protections. As Justice Sotomayor wrote in a concurrence to the 2012 *United States v. Jones* case, '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.'").

The pattern is clear: initially, we have privacy in our day-to-day affairs, but we have to be in person, as in a cash payment or a face-to-face conversation. Then technologies emerge that scale human action, but we lose privacy protections: a telephone call, a bank wire. Finally, technologies improve, restoring privacy without sacrificing scale, and the law catches up to protect citizens' privacy expectations: encrypted messaging, a bitcoin transaction.

American technological dynamism and constitutional law drove these changes. It's inevitable that financial transactions will be largely disintermediated, but it's not inevitable that America will lead this revolution as it did in the past.

Peer-to-peer financial systems are crucial for the future of the U.S. economy. If we don't allow their use and development by Americans, they will be used and developed overseas. Insisting on re-intermediating and surveilling peer-to-peer financial transactions would make the U.S. as noncompetitive as a country still relying on human switchboard operators for phone calls.

Nonetheless, as we will detail exhaustively below, several executive agencies are trying to do just that. The Internal Revenue Service ("IRS") is drafting rules that would force "unhosted wallet" software developers to go into the business of monitoring the users of their software against their will. The Department of Justice ("DOJ") in the Southern District of New York ("SDNY") is prosecuting software publishers as unlicensed money transmitters because unrelated users of their software have committed financial crimes. The Office of Foreign Asset Control ("OFAC") has banned Americans from using certain DeFi software tools even for entirely domestic and legitimate purposes. The Securities and Exchange Commission ("SEC") is using enforcement actions to fit cryptocurrency activities into traditional regulatory frameworks that require intermediaries.

These agencies pursue these regressive strategies without clear congressional direction. The IRS is contradicting the plain language of the Infrastructure Act in its broker rulemaking. The DOJ is offering unjustified interpretations of the Bank Secrecy Act ("BSA"), contradicting reasonable FinCEN guidance. OFAC is offering unjustified interpretations of the International Emergency Economic Powers Act ("IEEPA"). The SEC is stretching its jurisdiction through aggressive enforcement and an unconstitutionally expansive exchange rulemaking.

To better understand these missteps in DeFi policy, let's take each example in turn. In each case we'll explain what good regulation looks like and why the current approach has gone awry.

Treasury and the IRS's Broker Rulemaking

Coin Center has long advocated for Congress and the Treasury to treat trusted intermediaries in the cryptocurrency space identically to more traditional regulated financial services companies. This advocacy has included a call for clear guidance on third-party tax reporting obligations for cryptocurrency intermediaries.[10] We do not object to the imposition of third-party reporting obligations on true digital asset intermediaries so long as the imposed requirements mirror those imposed on traditional intermediaries.

A broker, as traditionally understood, is still a broker even if they are buying and selling cryptocurrencies on behalf of their customer rather than securities or more typical commodities. They are an agent of their customer in these sales or else they are a principal in a sale to the customer. Accordingly, the imposition of a recordkeeping and reporting requirement is reasonable under the relevant statute and the strictures of the United States Constitution. Therefore, we take no issue with sections of the ongoing broker rulemaking that would place true cryptocurrency intermediaries on equal footing with traditional brokerages.

However, Coin Center strongly objects to the Treasury Department's recent attempt to impose broker reporting obligations on persons who are not properly understood as brokers or middlemen and who are merely engaged in the publication or ongoing maintenance of software tools and websites or any mere relayers of cryptocurrency transaction messages.[11] In legal rather than technical terms, we object to the imposition of reporting obligations on any software or communications intermediaries who do not have any agency or agency-like relationship with the users of their published tools and websites, and who are in no position to know or collect personal information about those users. Indeed, we find that the extension of reporting obligations to these persons, among other legal defects, runs counter to the underlying statutory authority, the legislative history, and—most importantly—would violate the First Amendment rights of cryptocurrency software, data, and website publishers and the Fourth Amendment rights of both the publishers and the users of said software, data, and websites.

There are two areas of the proposed rulemaking that give rise to these statutory and constitutional issues: 1) the proposed new definition of "Digital Asset Middleman" and the several other new definitions providing guidance on the interpretation of that term, and 2) the

---

[10] See, *e.g.*, Jerry Brito, *Reps. Polis & Schweikert introduce Cryptocurrency Tax Fairness Act in Congress*, Coin Center, September 7, 2017, https://www.coincenter.org/reps-polis-schweikert-introduce-cryptocurrency-tax-fairness-act-in-congress/ (supporting a bill introduced in 2017 that directed the IRS to issue guidance on third-party tax reporting because "clear IRS guidance and informational reporting would be a lifesaver at tax time for cryptocurrency users.").

[11] *See* Internal Revenue Service, *Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions*, 88 F.R. 166, pgs. 59576-59659, https://www.govinfo.gov/content/pkg/FR-2023-08-29/pdf/2023-17565.pdf.

proposed redefinitions of the terms "effect" and "customer." These definitions taken together ultimately determine who must do reporting.[12]

The Treasury Department is bound to enact the law as made by Congress and is not free to go beyond that authority.[13] Broadening these definitions runs counter to the plain text of the statute as it was amended by the Infrastructure Investment and Jobs Act (hereinafter the Infrastructure Act)[14] and it also runs counter to the intent of Congress as found within the legislative history of that law's passage.

Irrespective of the statute, the Treasury Department is bound by the Constitution to ensure that its rules do not violate fundamental rights. Mandatory reporting provisions of any kind compel speech.[15] Any law that compels speech faces exacting scrutiny from the courts, meaning that the rule must be narrowly tailored to address a compelling government interest.[16] The proposed rule is not narrowly tailored and would subject far more persons to an onerous disclosure regime than is appropriate to ensure tax compliance. Moreover, applying a customer disclosure requirement to persons who have no customers in the traditional sense, to persons who merely publish software, websites, or other tools, compels them to write their tools in a manner that goes directly against their closely held political and social beliefs. In other words, demanding software developers to build software tools that intentionally violate the privacy of their users compels these developers not only to speak some factual disclosure about their software users but also to speak in a deeply expressive manner a viewpoint with which they do not agree.

Finally, the rule as applied to those who merely publish software, websites, or other tools, violates the Fourth Amendment rights of the persons obligated to make reports, even under the more lenient standards for warrantless administrative searches. Additionally, to the extent any obligated persons will be made to report any information about taxpayers that is not voluntarily provided by taxpayers for a legitimate business purpose, the proposed rule deputizes service

---

[12] For a more detailed description of the problems in the current proposed rule and our suggested alternative approach, *see* Coin Center, *Comment Letter on Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions* (Dep't of the Treasury Sept. 8, 2023), https://www.coincenter.org/comments-to-the-department-of-treasury-on-gross-proceeds-and-basis-reporting-by-brokers-and-determination-of-amount-realized-and-basis-for-digital-asset-transactions/.

[13] *See Federal Election Commission v. Ted Cruz For Senate*, 142 S. Ct. 1638, 1649 (2022) ("An agency, after all, 'literally has no power to act'—including under its regulations—unless and until Congress authorizes it to do so by statute.").

[14] *See Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58 (2021) https://www.govinfo.gov/app/details/PLAW-117publ58.

[15] *Americans for Prosperity Foundation v. Bonta*, 141 S. Ct. 2373 (2021)

[16] *Id.*

providers to engage in the warrantless search and seizure of taxpayer information in violation of the Fourth Amendment.

As of this hearing, the Treasury has only partially finalized its broker rulemaking: clarifying that custodial entities in the cryptocurrency space fit the definition of broker and need to do third party reporting. We are grateful for that clarity although it is several years overdue.[17] With respect to DeFI (which the IRS accurately refers to as non-custodial), the agency has further delayed offering a final rule, leaving these critical constitutional issues to another day and leaving innovators entirely uncertain about their obligations.

SDNY DOJ's Interpretation of Money Transmission

It has been the clear and consistent policy of FinCEN[18] since at least 2013 that cryptocurrency wallet developers and the users of those wallets are not money transmitters. Coin Center agrees with this policy and has lauded FinCEN for its frequent guidance and further clarifications in support of clear rules that achieve meaningful deterrence of crime while preserving innovation. So it has come as quite a surprise that the DOJ is suddenly intent on charging wallet developers criminally for unlicensed money transmission even if they exercise no actual control over the assets their users choose to secure with their software. This is an insidious development that appears to be nothing less than regulation by *criminal* enforcement.

Federal prosecutors have put forward this unprecedented interpretation of money transmission law in two recent cases: the April 26th unsealed Samourai Wallet indictment[19] and the DOJ's opposition to Roman Storm's motions to dismiss and suppress evidence in the Tornado Cash

[17] The IRS had the authority to offer this guidance at least as early as seven years ago when Coin Center worked with Reps. Polis and Schweikert to draft bipartisan legislation calling for guidance on 3rd party tax reporting in 2017. Jerry Brito, Reps. Polis & Schweikert introduce Cryptocurrency Tax Fairness Act in Congress, Coin Center, September 7, 2017, https://www.coincenter.org/reps-polis-schweikert-introduce-cryptocurrency-tax-fairness-act-in-congress/ (supporting a bill introduced in 2017 that directed the IRS to issue guidance on third-party tax reporting because "clear IRS guidance and informational reporting would be a lifesaver at tax time for cryptocurrency users."). And again in 2019, Coin Center and others including members of this committee urged the IRS to use existing authority to offer guidance. *See* Letter from Rep. Tom Emmer to IRS Commissioner Charles Rettig (Apr. 15, 2019), https://emmer.house.gov/2019/4/emmer-leads-bipartisan-blockchain-caucus-letter-irs-ahead-tax-day-urging. *See also* Coin Center, *Congress Sends Letter to IRS Regarding Urgent Need for Guidance on Crypto Taxes* (Sept. 1, 2023), https://www.coincenter.org/congress-just-sent-a-letter-to-the-irs-about-urgent-need-for-guidance-on-crypto-taxes/.

[18] FinCEN is the division of Treasury tasked with interpreting and enforcing anti-money-laundering laws for non-bank financial institutions, cryptocurrency businesses that qualify as money services businesses included.

[19] *United States v. Keonne Rodriguez & William Lonergan Hill*, S2 24 Cr. 82 (S.D.N.Y. 2024).

case, which was published the same day.[20] It is hard to know at this point if this is a deliberate attempt to abruptly change long-established policy through criminal enforcement, or if this is a significant disconnect between the Department of Justice and FinCEN. Either way, this is a disaster for the rule of law, due process rights for the accused, and our fundamental freedoms of speech and privacy. Here's a brief review of existing money transmission policy, and a detailed summary of the recent events.

The federal laws that regulate money transmitters are anti-money laundering (AML) statutes, specifically the Bank Secrecy Act and its amendments. These laws define a category of regulated businesses as "Financial Institutions" and also empower the Secretary of the Treasury to redefine that category as he sees fit. Because of this congressionally delegated power to expand the category, it is the implementing regulations of the Bank Secrecy Act (the "regulations") that actually define the law of who must and must not register as a money transmitter or other financial institution and practice Know Your Customer (KYC) guidelines, file reports with the government, and establish other AML controls.[21]

The regulations define a money transmitter as (1) any person who offers money transmission services, which the regulations define as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," and (2) "any other person engaged in the transfer of funds."

In the context of cryptocurrencies, that definition includes some ambiguities about whether cryptocurrency is "currency, funds, or other value that substitutes for currency." If cryptocurrency is "funds," then "any person engaged in the transfer" is a money transmitter. If, alternatively, cryptocurrency is "currency" or if it is "other value that substitutes" for currency, then any person who both "accepts" and "transmits" cryptocurrency is a money transmitter. A plain reading of the regulations suggests that cryptocurrency is a substitute for traditional currency and, therefore, a person is a money transmitter if they both accept and transmit that cryptocurrency as a business for other people. In other words, if someone has actual control over another person's cryptocurrency and uses that control to move that person's

[20] *United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government's Opposition to Defendant Roman Storm's Pretrial Motions) available at https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf

[21] For a deeper analysis of the statutory authority behind anti-money laundering policies and potential constitutional separation of powers issues therein, *see* Peter Van Valkenburgh, *Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act 1.0*, November 2023 available at https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/

cryptocurrency to another person or location they are a money transmitter. This has been the controlling law since before cryptocurrency existed and it has never been amended or overruled by Congress, the courts, or regulation. As we'll discuss, the minor ambiguity over whether cryptocurrency is currency, funds, or value that substitutes for currency was resolved early in the history of crypto regulation by FinCEN.

In 2013, FinCEN released its first "virtual currency" guidance.[22] In it, FinCEN confirmed that cryptocurrency (virtual currency as they called it) is "value that substitutes for currency" and that it is not "funds" or "currency" itself (hence "*virtual* currency"). In a footnote it also clearly stated that it does not consider virtual currency to be "funds" because doing so would trigger prepaid access regulations that FinCEN felt were inapplicable to cryptocurrency activities:

> If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency."[23]

FinCEN went on to explain that mere users of virtual currencies are not money transmitters and in a subsequent administrative ruling found that software developers are also not money transmitters: "The production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, *even if the purpose of the software is to facilitate the sale of virtual currency.*" [emphases added].[24]

Coin Center and others lauded this clear statement of policy and over the following years pushed for additional clarity on the lingering question of partial control over virtual currency,

---

[22]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[23] *Id.*
[24] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf.

as exists in the case of multisig wallets and time-locked contracts like those in the Lightning Network.[25] In response FinCEN published additional guidance in 2019.[26]

The 2019 Virtual Currency Guidance clearly articulated that partial control over virtual currency was insufficient to classify wallet developers as money transmitters because: "the person participating in the transaction to provide additional validation at the request of the owner *does not have total independent control over the value*."[27]

Coin Center once again lauded FinCEN for clearly articulating a policy that rightfully required only custodial cryptocurrency businesses to license and be subject to federal money transmission regulations.[28] Even if we set aside these guidance documents and administrative rulings, however, a plain reading of the underlying binding rules also shows that money transmission in cryptocurrency only happens if someone both "accepts" and "transmits" cryptocurrency on behalf of another person.[29] In other words, for as long as cryptocurrency has existed, the law has been unambiguous: non-custodial cryptocurrency developers are not money transmitters.

On April 26th 2024 an indictment was unsealed[30] that accused the developers of Samourai Wallet (a Bitcoin wallet that uses CoinJoin transactions to enhance user privacy[31]) of unlicensed money transmission among other charges. For the purpose of this discussion we will not discuss the charge of conspiracy to launder money. That charge is fact-dependent and does not necessarily rely on the developers offering a custodial rather than non-custodial wallet service. The defendants may have, as alleged, operated a centralized server to coordinate CoinJoin

---

[25] The lightning network is a scaling solution to reduce the cost of making bitcoin transactions without introducing trust or reliance on third-parties. *See* Coin Center, *The Lightning Network* (2023), https://www.coincenter.org/education/key-concepts/lightning-network/.

[26] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[27] *Id.*

[28] Coin Center, *FinCEN's New Cryptocurrency Guidance Matches Coin Center Recommendations* (May 9, 2019), https://www.coincenter.org/fincens-new-cryptocurrency-guidance-matches-coin-center-recommendations/.

[29] 31 C.F.R. § 1010.100(ff)(5) (2023) ("The term 'money transmission services' means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.").

[30] *United States v. Keonne Rodriguez & William Lonergan Hill*, S2 24 Cr. 82 (S.D.N.Y. 2024).

[31] Coin Center, *What Are Mixers and Privacy Coins?* (2023), https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/.

transactions. However, the Samourai Wallet did not afford the developers or any other third-parties actual independent control over bitcoins secured by users of the wallet software. Under a plain reading of the regulations and especially in light of the FinCEN guidance and administrative rulings, the developers of Samourai Wallet did not have "total independent control" over any user funds and therefore were thus not money transmitters.

Also on April 26th, the prosecution in the Tornado Cash criminal case against developer Roman Storm offered a reply brief that responded to the defense's earlier motion to dismiss. A substantial subsection of the reply is titled "Section 1960 Does Not Require the Business to Have Control of the Funds."[32] There "Section 1960" is referring to the section of the criminal code that makes it illegal to operate an unlicensed money transmitting business.[33] The brief spends pages arguing that the definition at 1960 is broader than the actual definition in the Bank Secrecy Act and the regulatory definition offered by the regulator that we discussed above. It would be a blatant violation of due process rights if you could be charged under a criminal definition of "unlicensed" conduct even if the actual regulatory definition of which conduct requires a license clearly did not include the conduct in which you engaged. Nonetheless this is what the brief argues.

The brief goes on to argue that the Tornado Cash developers are culpable because the Tornado Cash software "caused cryptocurrency to pass from one place to another on the Ethereum blockchain every time a customer requested a deposit or withdrawal."[34] This is a massive overreach. By the prosecution's absurdly broad and unsupported standard, every functioning cryptocurrency wallet and smart contract is "doing" money transmission and every developer is engaged in unlicensed money transmission.

Eventually the reply brief reaches the regulatory definition but it ignores all of the existing guidance that we outlined above and interprets the "funds" section of the definition with absurd breadth, arguing that the law simply asks if someone is "any person engaged in the transfer." This entirely ignores the fact that FinCEN has previously articulated that virtual currency is not "funds." To illustrate their point about "control" being non-essential, the prosecution makes a comparison to parcel delivery:

---

[32] *United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government's Opposition to Defendant Roman Storm's Pretrial Motions) available at https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf

[33] 18 U.S.C. § 1960.

[34] *United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government's Opposition to Defendant Roman Storm's Pretrial Motions) available at https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf

> Consider the example of a business that accepts parcels of cash from criminals and moves the money by courier to locations overseas, perhaps the archetypal Section 1960 violation. Under the defendant's theory, such a business could escape liability by the simple expedient of only accepting cash in locked parcels, as long as its customers did not give it the keys to unlock the parcels. Then, it could claim, it never had "control" over the funds.[35]

This brief section is indicative of the low-ball tactics being employed by the prosecution. First note the immediately prejudicial nature of the parcel service, it "accepts parcels of cash from *criminals*." If Tornado Cash was a parcel service it certainly didn't only accept parcels from criminals. Coin Center happily used Tornado Cash to accept legitimate donations.[36] Second, the comparison proves exactly the opposite of what the prosecutors want it to prove. A delivery service that cannot access the underlying contents of the parcels it delivers is *plainly and clearly not a money transmitter*. First of all, if you can't open the parcel how do you even know what is in it? Can you be guilty of unlicensed money transmission if you were told you were only moving boxes of canned Spam and had no way to open the boxes? Second, FinCEN has expressly ruled that armored car businesses that are "limited to secure transportation of currency" *are not money transmitters under their rules*.[37] Sadly, the prosecution may dismiss that administrative ruling just as they have dismissed the otherwise comprehensive and clear guidance that FinCEN has offered on virtual currencies.

As we have argued in our own civil lawsuit to remove the Tornado Cash smart contracts from the OFAC list[38] and in our amicus brief in this criminal case,[39] no third party including the Tornado Cash developers ever had any actual control over the cryptocurrency that users of the

---

[35] *Id.*

[36] *See Brief of Amicus Curiae Coin Center in Support of Defendant Roman Storm's Motion to Dismiss* at 10-11, United States v. Roman Storm, No. 23 Cr. 430 (S.D.N.Y. Apr. 5, 2024), https://www.coincenter.org/app/uploads/2024/04/Coin-Center-Amicus-Brief-filed.pdf ("Coin Center has used Tornado Cash to privately accept donations that support our non-profit mission. We have brought a lawsuit to have OFAC remove the Tornado Cash pool addresses from the sanctions list so that we can continue to use them for that purpose and so that other Americans can use them for any legitimate privacy purposes. We have co-plaintiffs in that lawsuit who wish to use Tornado Cash to be privately paid their salary and who have used it to privately make donations to the war effort in Ukraine without becoming targets of Russian cyber attacks.").

[37] Financial Crimes Enforcement Network, *Definition of Money Services Business (Money Transmitter/Currency Dealer or Exchanger)* (2004), https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-money-services-business-money.

[38] Coin Center, *Coin Center Is Suing OFAC Over Its Tornado Cash Sanction* (Oct. 12, 2022), https://www.coincenter.org/coin-center-is-suing-ofac-over-its-tornado-cash-sanction/

[39] Coin Center, *Coin Center Files a Court Brief in Defense of Tornado Cash Developer* (Feb. 10, 2023), https://www.coincenter.org/coin-center-files-a-court-brief-in-defense-of-tornado-cash-developer/.

tool owned. Under clear and long established FinCEN guidance and under any common sense reading of the underlying law, these developers are not money transmitters. Nonetheless the prosecution persists unjustly.

We are grateful that Senators Lummis and Wyden have expressed similar concerns over these overzealous criminal prosecutions and their muddling effect on FinCEN policy. We hope members of this subcommittee will add their voices to the effort and persuade the DOJ to drop these unreasonable charges.

OFAC Privacy Tool Bans

Sanctions are an important part of our foreign policy toolset. Coin Center does not object to the use of sanctions against foreign persons who are promoting terror or international crime including if they are doing so by sending and receiving cryptocurrencies to or from cryptocurrency addresses that they control. We do not, however, support OFAC's attempt, herein described, to abuse sanctions laws in order to block ordinary Americans from using tools that protect their legitimate privacy interests.

Privacy is not the default on Ethereum or in most of DeFi generally. If you do your job using these technologies, your co-workers can see your salary. If you donate to a political cause, the opponents of your cause can see your contribution. If you are a celebrity on these networks, your fans see not just your publicized activities but also your private personal accounts and net worth. Privacy is *normal* for a salaried employee, a charitable donor, even a celebrity, but privacy is not normal if you do these things on Ethereum *unless you use a tool like Tornado Cash*. In August of 2022, the U.S. Treasury unilaterally and extralegally made it a crime for Americans to use Tornado Cash for any purpose.[40]

Later that fall, Coin Center, along with a group of normal privacy-seeking American workers, donors, activists, and public figures, filed a lawsuit against the Treasury Department to keep privacy normal, to delist Tornado Cash privacy tools from sanctions, and to enjoin Treasury from enforcing against ordinary Americans exercising their self-evident and basic rights to privacy.[41] Our lawsuit is currently on appeal in the 11th Circuit and oral argument is scheduled for November 18th.

[40] Complaint, Coin Center v. Yellen, No. 3:22-cv-20375 (N.D. Fla. Oct. 12, 2022), https://www.coincenter.org/app/uploads/2022/10/1-Complaint-Coin-Center-10-12-22.pdf.
[41] *Id.*

Our lawsuit makes four claims. First, Congress gave the president *very specific* powers when it passed the International Emergency Economic Powers Act upon which Treasury's sanction rules are based: sanctions can block U.S. persons from transacting with a foreign person or majority foreign entity or the property of that person or entity. When we or our co-plaintiffs use the Tornado Cash tools, we do so as normal, privacy seeking Americans. We do not engage in any transactions with any foreign person or entity or their property. Instead, we are using immutable and widely available software on the Ethereum blockchain to move our own valuables from one place in cyberspace that is fully under our control to another place that we also control. At no point are we relying on any third party for these transactions and at no point are we transacting with a sanctioned person. Plainly, given the specific powers granted to the Treasury Department by Congress, these are not the kinds of activities that can be censored or blocked. The Tornado Cash sanction was, therefore, made in excess of statutory authority and must be set aside.[42]

Second, even Treasury's own regulations and past executive orders limit the applicability of sanction controls to transactions with persons, entities, or their property.[43] The Tornado Cash sanction was made without statutory and also without regulatory authority. It was made contrary to law.

Third, in sanctioning Tornado Cash tools, the Treasury failed to consider the collateral consequences of its actions or manifest any awareness of, or justification for, their significant deviation from previous sanctions policies. Their actions were arbitrary and capricious. Since the sanction, Americans have had money trapped in a smart contract without any due process; they've been attacked by malicious continued use of the smart contract that saddles them with indefinite reporting requirements or else criminal penalties through no fault of their own. Meanwhile, the Treasury has issued statements that directly contradict their own rules, and scant public clarity has been offered in the face of real public confusion and harm.[44]

Fourth, Americans have had their associational activities chilled as once private donations to political causes must now be made public on chain. Our American system relies on certain essential and self-evident rights. Among them, that you can meet with others to petition the government and contribute to groups and organizations that will further those advocacy efforts. Key to our freedom of association is the right to make these donations in private, to not be forced to disclose to the government or any third party a list of the people who believe in your cause. Coin Center, among many non-profits, relied upon Tornado Cash for private

[42] *Id.*
[43] *Id.*
[44] *Id.*

donations. Another of our co-plaintiffs relied upon Tornado Cash to organize substantial support for the defense of Ukraine. Subjecting these transactions to public scrutiny would not only chill the protected activities of donors, it would put those donors and activists in real danger of Russian reprisals.

For all these reasons and more, Coin Center opposes Treasury's extra-legal usage of its sanctions authority to strip U.S. persons of access to software tools that are necessary to protect our basic privacy needs as we go about our lives. We hope that members of this committee will investigate Treasury's extra-legal actions and ensure both that OFAC's authority is limited to what Congress intended, and that Americans' rights are not infringed by these actions.

SEC Enforcement Actions and Exchange Rulemaking

In 2016, Coin Center was one of the first organizations to publish a detailed report on why certain so-called "initial coin offerings" ("ICOs") may be unlicensed securities issuance in contravention of the Securities laws.[45] Since 2016 we have recommended that the SEC "take action necessary to protect investors against cryptocurrencies well-fitted to the Howey test, presenting greater risks to users" such as "closed-source or low-transparency cryptocurrencies," "open but heavily marketed pre-sales or sales of pre-mined cryptocurrencies with a small and non-diverse mining and developer community" and "cryptocurrencies with permissioned ledgers or a highly centralized community of transaction validators."[46] In short, we are not in favor of and have never advocated for a fully hands-off approach to investor protection in the cryptocurrency space. We have also worked with Members of this Committee and others in Congress to draft new legislation that would impose reasonable market structure oversight on custodial cryptocurrency exchange platforms to ensure investor protection.

The SEC, however, has recently eschewed any such nuanced analysis of securities laws in favor of an imperial approach toward their jurisdiction. They have brought dubious enforcement actions and have an ongoing rulemaking that would classify mere software developers as national securities exchanges bound to registration and oversight.

The two best examples of recent inappropriate and overbroad prosecutions from the SEC are the claims against Coinbase that their noncustodial wallet product offers unlicensed brokerage services and the claims against Consensys that their metamask wallet does the same. The

[45]Peter Van Valkenburgh, *Framework for Securities Regulation of Cryptocurrencies 2.0*, August 2018. (Version 1.0 of this report was published in 2016 and our in-person briefings with SEC staff covered these recommendations as early as 2015).
[46] *Id.*

Coinbase wallet claims were rightfully dismissed by Judge Failla of the Southern District of New York.[47] The Consensys claims have yet to be addressed on motion to dismiss.

The ongoing Consensys case in particular is highly fact dependent and deals with new technologies, such as liquid staking tokens, that will present various questions of first impression to judges. It's deeply unfortunate that the SEC has decided to charge into this ambiguous area with an aggressive surprise enforcement action rather than first offering clearer guidance and rulemakings that give the public and any potential defendants the benefit of due process and the rule of law. Crypto wallets like Consensys' Metamask are essentially just user interfaces; they are to blockchain networks what the desktop web browser is to the world wide web. If we'd taken the SEC's current enforcement approach back in the 1990s, federal agents would have been raiding Netscape's offices, and arresting developers because of web content their users happened to visit while using Netscape Navigator. The result would be (and is) holding the wrong people responsible for content that may not even be illegal. The result is anti-innovation and seeks centralized control over speech and discourse.

The SEC's aforementioned rulemaking is intended to expand the definition of "exchange" in order to encompass additional financial services organizations.[48] The way it does so, however, would create an inappropriately broad standard for registration that would impose an unconstitutional prior restraint on the protected speech activities of countless software developers and technologists.

The existing definition of exchange is conduct-based. One is an exchange if one engages in certain specified conduct: One "uses" methods to bring together "orders." The newly proposed definition is speech-based: One is an exchange if one publishes speech that brings other persons together and affords them a set of rules enabling them to trade, i.e. if one merely "makes available" a "communication protocol" such that other people come together and trade.

While the constitutionality of the existing regulatory definition has not been tested in court, the fact that it places a prior restraint on conduct ("using … methods") rather than on speech ("making available … protocols") suggests that it could survive constitutional scrutiny. Laws regulating conduct, even if it is expressive conduct (e.g. flag burning or nude dancing) and even

[47] SEC v. Coinbase, Inc., No. 1:23-cv-04738, 2024 WL 1234567 (S.D.N.Y. Mar. 27, 2024)
[48] Securities and Exchange Commission, *Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities*, 87 FR 15496, pgs. 15496-15696, March 18, 2022, https://www.federalregister.gov/documents/2022/03/18/2022-01975/amendments-regarding-the-definition-of-exchange-and-alternative-trading-systems-atss-that-trade-us.

if the law impacts some speech incidental to conduct (e.g. a lawyer mostly speaks but must be licensed to practice law), are judged under an intermediate scrutiny standard and are often found constitutional despite their tendency to limit otherwise protected expression. By contrast, laws regulating speech qua speech are judged under a strict scrutiny standard and are rarely found constitutional.

The Supreme Court has already ruled against similar unconstitutional overreach by the Commission in the context of the Investment Advisers Act,[49] and is primed to do so again given recent opinions dealing with data brokers and commercial speech.[50] The chilling effect inherent in imposing an overly broad standard for registration, matched with severe penalties for non-compliance, will lead many creative and inventive Americans to self-censor.

The SEC has yet to finalize this rulemaking and we hope they will abandon this unconstitutionally overbroad definition in the final rule. If this rulemaking were to move forward, Congress can exercise its appropriate oversight function to reject this rule. Congress can also provide important clarifications to securities laws, like those included in the Securities Clarity Act and FIT 21, which are already being confirmed as rational approaches under existing law in several recent court cases.[51]

Conclusion

Congress has a pivotal role to play in preserving American dynamism. Some members have already begun to push back against these unlawful and unconstitutional intrusions. The Blockchain Regulatory Certainty Act, the Keep Your Coins Act, FIT21, and other initiatives seek to clarify the legal landscape and leave room for innovation. If the American Constitution is to be preserved, the Court should push back. Revive our right against warrantless search by overturning *Miller*, and protect our First Amendment rights to publish software.

---

[49] *Lowe v. Securities & Exchange Commission*, 472 U.S. 181, 236 (1985).
[50] *Sorrell, et al. v. IMS Health Inc., et al.*, 564 U.S. 552 (2011).
[51] See e.g., SEC v. Ripple Labs, Inc., No. 1:20-cv-10832, 2023 WL 4508821 (S.D.N.Y. July 13, 2023). Judge Analisa Torres granted partial summary judgment in favor of Ripple, ruling that certain XRP sales did not violate securities laws, but institutional sales did. The SEC's request for $1.07 billion in disgorgement was reduced to $125 million in penalties during the remedies phase. See also Judge Torres's distinction between institutional and secondary market sales. *See also*, SEC v. Payward Ventures, Inc. (Kraken), No. 3:23-cv-00634 (N.D. Cal. Aug. 23, 2023). Judge William Orrick ruled against Kraken's motion to dismiss, allowing the SEC's case regarding its staking-as-a-service program to proceed, while rejecting the SEC's claim that digital asset securities were a special form of security, *and SEC v. Binance Holdings Ltd.*, No. 1:23-cv-01599 (D.D.C. June 29, 2024). Judge Amy Berman Jackson ruled that the SEC's major charges against Binance for unregistered securities offerings and other regulatory breaches could proceed, although some claims related to secondary market activities were dismissed.

My organization Coin Center is also dedicated to preserving American dynamism. We are here to educate members of Congress and the Executive Branch about these technologies, advocate for reasonable regulations, and preserve constitutional rights, as we are doing through the two challenges to regulatory overreach that we've so far brought in the courts.

This isn't a lawless future I'm describing. It's a future where the law is not abused to force Americans to use outdated tools or ban them from building better ones. It's un-American to tell an inventor she needs state-approval before publishing words or code describing her invention. It's very American to take her to court if she lied about what the invention would do or used the invention to commit a crime. We need to focus on *ex-post* regulatory efforts, such as fraud, contracts, torts, and unfair and deceptive acts and practices prosecution. This is a significant departure from our traditional financial regulatory structure, focused as it is on *ex ante* licensing, registering, and chartering. However, it is the only regulatory structure that can be aimed at DeFi without compromising our country's technological dynamism and our Constitutional right against prior restraints on speech. I appreciate the Committee's time and look forward to addressing any questions you may have.