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"

CC:PA:LPD:PR (REG- 122793-19),
Room 5203, Internal Revenue Service,
P.O. Box 7604, Ben Franklin Station,
Washington, DC 20044

[REG-122793-19] RIN 1545-BP71

November 9, 2023

To whom it may concern:

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.

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.[1] 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

[1] 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.").

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 this rulemaking that would place true cryptocurrency intermediaries on equal footing with traditional brokerages.

However, Coin Center strongly objects to the Treasury Department's attempt in this rulemaking 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.[2] 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 proposed redefinitions of the terms "effect" and "customer." These definitions taken together ultimately determine who must do reporting.

The Treasury Department is bound to enact the law as made by Congress and is not free to go beyond that authority.[3] 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)[4] and it also runs counter to the intent of Congress as found within the legislative history of that law's passage.

---

[2] *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.

[3] *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.").

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

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

To remedy these issues, we propose a much simpler redefinition of "broker" that merely clarifies that the existing broker reporting requirements now also explicitly include brokers effecting sales of digital assets. This approach would be technology neutral, simpler to administer, and requires none of the complicated newly defined terms in the current proposal. It also, unlike the current proposal, mirrors the intent of Congress and respects the fundamental Constitutional rights of Americans.

At the end of the first sentence of the broker definition the phrase, "including sales of digital assets," should be included. The rest of that definition can then be left unchanged:

> The term broker means any person (other than a person who is required to report a transaction under section 6043 of the Code), U.S. or foreign, that, in the ordinary course of a trade or business during the calendar year, stands ready to effect sales to be made by others**, including sales of digital assets**.[5]

Under this approach, there would then be no need to define "digital asset middleman," "facilitative service," "in a position to know," "nature of the transaction," "held in a wallet or account," "hosted wallet," "unhosted wallet," or any of the other digital asset specific terms

[5] *Supra* note 2, at pg. 59631, bolded words added.

proposed. There would also be no need to craft specific rules for digital asset sales as compared with regular asset sales.[6]

The terms "effect" and "customer" should not be redefined in this rulemaking as there is no indication that Congress intended to change these terms. These terms in their original form create a reasonable and justiciable test for when a person is, in fact, acting as a broker with respect to traditional assets. That same test should apply in the context of digital assets.

This alternative approach would vastly simplify an important amendment to an already complex tax code, maintain a technology neutral standard for broker reporting, and—as explained in the remainder of this comment—honor the intent of Congress as evidenced in the plain text of the infrastructure act and the legislative history of its drafting. It will also save this rule from unconstitutionality.

The proposed rule goes beyond the statutory authority and a broader interpretation of the statutes is contradicted by the legislative history

The existing regulatory broker definition hinges on whether a person "effects" sales for "customers."[7] Both the term "effect" and the term "customer" are defined such that coverage of the broker definition is limited to persons who are either agents of the customer, principals in a sale to the customer or persons obligated to pay the customer the proceeds of the sale. Those definitions are in full, emphases added:

> (10) The term effect means, with respect to a sale, to act as:
>
> > (i) An **agent** for a party in the sale wherein the nature of the agency is such that the agent ordinarily would know the gross proceeds from the sale; or
> >
> > (ii) A **principal** in such sale.[8]

And:

> (2) The term customer means, with respect to a sale effected by a broker, the person (other than such broker) that makes the sale, if the broker acts as:
>
> > (i) An **agent** for such person in the sale;

[6] While not the focus of this comment, we argue that the types of information collected and reported by brokers dealing in digital assets should be identical to the types of information collected and reported by brokers dealing in traditional assets. The proposed rule contemplates the collection of a large amount of digital asset specific information that is violative of personal privacy and not necessary to achieving the policy objective of efficient tax administration.

[7] 26 CFR § 1.6045-1.

[8] *Id.*, emphasis added.

(ii) A **principal** in the sale; or

(iii) The participant in the sale **responsible for paying** to such person or crediting to such person's account the gross proceeds on the sale.[9]

Hereinafter, for brevity, we will refer to this agent-of, principal-for, or payor-to relationship as a "customer agent or principal."

That existing standard and its focus on an agency relationship is in line with the plain meaning of the term broker, *e.g.* from Webster's dictionary, emphasis added:

> Broker: one who acts as an intermediary: such as (a) an **agent** who arranges marriages, (b) an **agent** who negotiates contracts of purchase and sale (as of real estate, commodities, or securities)[10]

The Infrastructure Act amended the definition of broker to include also, emphases added, "any person who (for consideration) is responsible for regularly providing any service **effectuating** transfers of digital assets **on behalf of another person**."[11]

Congress chose to use the same verb, "effectuating," as the existing agency-focused regulatory definition, "effect," and emphasized the same principal-agent relationship with the plain language "on behalf of another person."

The plain meaning of the amendment, therefore, directs the Treasury Department to maintain the existing scope of the definition with respect to types of activities that trigger reporting obligations. Those activities should continue to be understood as being an agent for a customer and effecting sales on that customer's behalf or being a principal in a sale to a customer. The amendment merely expands and clarifies the broker definition with respect to the new *objects* of those otherwise similar activities: from agency in sales of traditional securities and commodities to cover also agency in transfers of digital assets. The plain text does not support an expansion of the definition to a new range of activities beyond the existing customer-agent or principal standard. It does not support expansion of the broker definition to persons who are mere communications intermediaries, software developers, or other persons who merely facilitate the activities of persons buying or selling digital assets but do not act as the person's agent in a transaction or as a principal in a sale to that person.

---

[9] *Id.*, emphasis added.
[10] Merriam-Webster Dictionary, "broker," accessed October 25, 2023, https://www.merriam-webster.com/dictionary/broker, emphasis added.
[11] *Supra* note 1.

Indeed, the legislative history shows that Congress explicitly declined to expand the range of activities covered by the definition beyond the customer-agent or principal standard.[12] In an early discussion draft of the Infrastructure Act the text of the definition included several new activities beyond the existing definition:

> (D) any person who (for consideration) regularly provides any service or application (even if noncustodial) to facilitate transfers of digital assets, including any decentralized exchange or peer-to-peer marketplace.[13]

However, this language was explicitly rejected by Congress during a heated debate that delayed passage of the bill.[14] The earlier text differs from the final version in several important ways, all of which underscore a refusal by legislators to depart from the *customer agent or principal* standard:

1. The earlier draft had a vague term "facilitate" rather than the "effectuate" standard that references the existing regulatory definition of "effect." That existing regulatory definition is limited to customer-agents or principals in sales.

2. The earlier draft included both providing a "service" as well as an "application (even if noncustodial)" while the final text only included "service." This indicates that Congress was ultimately unwilling to extend obligations to persons who merely provide others with software tools for trading.

3. The earlier version did not include "on behalf of another person" and the final text did, once again indicating that Congress was unwilling to extend reporting obligations to persons who were not acting on behalf of others, *i.e.* involved in an agency-like relationship with their customers.

4. The earlier version explicitly included persons who provide services or applications that are generally understood as lacking an agency relationship between the service provider and the user. Specifically the earlier version included providers of tools where users act

---

[12] See *Chickasaw Nation v. United States*, 534 U.S. 84, 93 (2001) ("We ordinarily will not assume that Congress intended 'to enact statutory language that it has earlier discarded in favor of other language.'").
[13] Ella Beres, "Crypto Tax Enforcement Update: The New Broker Definition in the Information Reporting Requirement Provision of the Infrastructure Bill Aims to Exclude Node Operators, Miners, and Validators," Davis Wright Tremain LLP, August 8, 2021, https://www.dwt.com/insights/2021/08/crypto-tax-enforcement-update. *See also* the full text of the discussion draft on file with author, available at https://drive.google.com/file/d/1wHs-pQR2bmGMzC-bkvHvnKCF89NZ4l1B at 2306.
[14] Andrea O'Sullivan, "How a Sneaky Crypto Crackdown Plot Blew Up the Infrastructure Bill," *Reason*, August 10, 2021, https://reason.com/2021/08/10/how-a-sneaky-crypto-crackdown-plot-blew-up-the-infrastructure-bill/.

only with other users such as "decentralized exchange" and "peer-to-peer marketplace." All of these terms were struck in the final version of the act.

The final language of the infrastructure act was the result of extensive debate and a deliberate choice by Congress to exclude several entities who were implicated by the draft language. This choice is evidenced by statements from the bipartisan group of Senators that introduced the final language. On the floor of the Senate, Senator Portman explained his reservations with the original draft language (emphasis added):

> In particular, we want to be sure **miners and stakers and others** now or in the future who play a key role by validating transactions, or sellers of hardware or software for digital wallets, or node operators, or **others who are not brokers** are clearly exempted.[15]

Moreover, Senator Portman articulated the core question addressed by the legislation and characterized the consensus answer in the Senate as simply mirroring existing standards for brokers of traditional financial instruments to persons performing the same activities with cryptocurrency (emphases added):

> The question is who should issue that 1099 in a cryptocurrency context. Again, the consensus is that it should be the brokers of cryptocurrency, **just as it is for stocks and bonds and other financial instruments**.[16]

Additionally, after passage of the Act, six Senators who were key to narrowing the original language wrote a letter that underscored the need to avoid overbroad interpretation:

> Now that this bill has become law, Congress has a responsibility to ensure that it is implemented effectively and in accordance with congressional intent. … As Senator Portman and Senator Warner articulated in a colloquy on the floor of the Senate on August 9, 2021, "[t]he purpose of this provision is not to impose new reporting requirements on people who do not meet the definition of brokers."[17]

Finally, a bipartisan group of House members wrote a letter urging Treasury to avoid an inappropriately broad interpretation of the much-debated final text:

---

[15] Congressional Record Vol. 167, No. 143 (Senate - August 8, 2021) at S6042, https://www.congress.gov/congressional-record/volume-167/issue-143/senate-section/article/S6034-2?s=2&r=1.

[16] *Id.*

[17] Letter to Treasury Secretary Janet Yellen, Sen. Mark Warner et al., December 14, 2021, https://www.warner.senate.gov/public/index.cfm/2021/12/warner-portman-bipartisan-colleagues-urge-treasury-secretary-to-implement-cryptocurrency-provision-in-bipartisan-infrastructure-law-effectively.

> These provisions were the subject of much debate. Any rulemaking or guidance that fails to appropriately interpret these provisions will damage the privacy of American taxpayers and stifle innovation through rising compliance costs and unnecessary regulatory burdens.[18]

Therefore, as debated on the floor and as embodied in the final text, the infrastructure act did not expand the category of activities that constituted *being a broker*, it simply made clear that third party reporting would apply to persons brokering, in the traditional sense, digital asset transactions.

Treasury's rulemaking is therefore faithful to the legislative intent and the text of the statute only in those sections where it describes applying third-party reporting requirements to digital asset brokerage services that are otherwise identical to traditional brokerage services but for the type of asset being brokered. This category correctly includes professional custodians (*e.g.* "hosted wallet providers"[19]) and it also includes some non-custodial entities who are, nonetheless, in a position of trust because their business involves a contractual, fiduciary, or agency relationship with their customer that goes beyond the mere publishing or communication of software or information (*e.g.* underwriters and escrow providers). Treasury's rulemaking departs from the statutory authority and legislative intent when it seeks to further expand the term broker beyond traditional agency-like relationships and into the realm of mere information communication or software publishing.

As such, to avoid overstepping the clear limits of statutory authority designated by Congress, the Treasury Department should merely clarify in its regulations that the existing definition of broker includes sales of digital assets. As argued above, the Treasury should, at the end of the first sentence of the broker definition, add the phrase, "including sales of digital assets." No other changes to the regulations are necessary.

Failure to cabin the reporting requirement to customer agents or principals in sales of digital assets would not only contravene the stated intent of Congress, it would also raise grave doubts about the constitutionality of the reporting regime. We will now turn to a discussion of why the broader definitions proposed in this rulemaking unreasonably curtail the First and Fourth Amendment rights of U.S. persons.

---

[18] Letter from Rep. Patrick McHenry to Treasury Secretary Janet Yellen, December 14, 2022, https://financialservices.house.gov/uploadedfiles/2022-12-14_rm_mchenry_letter_to_yellen_final.pdf.
[19] *Supra* note 2, pg. 59576.

The proposed rule as applied to non-agent or non-principal brokers is an unconstitutional speaker- and viewpoint-based compulsion to speak

The proposed rule directs brokers to make disclosures to the IRS and the taxpayer. Mandatory reporting and disclosure provisions of any kind compel speech.[20] Any law that compels speech faces, at least, exacting scrutiny from the courts.[21] Exacting scrutiny requires that the rule be narrowly tailored to address a compelling government interest.[22] The proposed rule creates disclosure obligations for persons who do not in the ordinary course of their business have any reason to collect and report the requested information. The rule is therefore not narrowly tailored; it would subject far more persons to an onerous disclosure regime than is appropriate to promote tax compliance.

Moreover, applying a customer disclosure requirement to persons who have no customers in the traditional sense, to persons who merely publish software (including websites and smart contracts[23]), compels them to write their software tools in a manner that goes directly against their closely held political, moral, and social beliefs. In First Amendment terms, demanding software developers build software tools that intentionally violate the privacy of their users compels these developers not only to speak some factual disclosure about the users of their software, but also to speak in a deeply expressive manner by crafting new software tools with alternative functionality and significantly compromised security and privacy guarantees. That compulsion to write software of a certain content and capability and to never write software of

---

[20] *Americans for Prosperity v. Bonta*, 594 US _ (2021).

[21] *Id.* at 2383. ("We have since settled on a standard referred to as 'exacting scrutiny.' Under that standard, there must be a substantial relation between the disclosure requirement and a sufficiently important governmental interest.").

[22] *Id.*

[23] These things too are software. Regularly publishing software tools, including graphical user interfaces, to a website or to a blockchain does not somehow make the activity something other than mere publishing. This does not, of course, mean that it is inappropriate to, for example, regulate banks when they have no branches and do all their business through websites. The banks in this hypothetical do many things in addition to publishing software on their websites. Among those additional things is the creation of legally binding contractual, agency, and/or fiduciary relationships between the banker and the customer. Those activities can and likely should be regulated. Mere publication and distribution of software to the general public, however, does not create a contractual, agency, or fiduciary relationship between the publisher and her audience. Nor does control over a particular publishing platform or publishing medium, e.g. a website domain name or an ethereum smart contract address, create such relationships. If the First Amendment does not protect the New York Times when it publishes regularly to nytimes.com, then it would offer very little protection to 21st Century speakers at all. Indeed, as discussed later in this comment, the Supreme Court has specifically held that the act of publishing websites, even if performed for profit, is protected as "pure speech." *See 303 Creative LLC v. Elenis*, 600 U.S. __ (2023) (holding that "images, words, symbols, and other modes of expression" is protected as "pure speech" and not as expressive conduct).

a differing content and capability is a compulsion to express a certain viewpoint about information security and privacy. That mandatory viewpoint is one with which most targeted speakers do not agree. It is, in total, a compelled speech order that imposes viewpoint discrimination on speakers. It is unequivocally unconstitutional under longstanding Supreme Court precedent.

The Supreme Court has consistently struck down laws that compel speakers to voice viewpoints with which they do not agree.[24] Indeed, even in the context of viewpoint neutral regulations that compel speech, the Court has expressed extreme skepticism.[25] This area of constitutional law is under-discussed in legal academia and may not be immediately intuitive to policymakers. Several counter arguments to the unconstitutionality of the provision, therefore, warrant a full rebuttal within this comment for the record. Alongside a general unpacking of the relevant constitutional standards, we will address the following counter-arguments:

1. The mandated reports are not protected speech activities because they are not expressive; therefore their compulsion does not raise First Amendment concerns.

2. The speech in question is commercial in nature and the speakers are typically corporations; therefore the rules warrant lesser First Amendment scrutiny.

3. The regulation in question is a reasonable prophylactic against lawbreaking. It only burdens questionable speech that supports criminal activity and therefore the regulations warrant lesser constitutional scrutiny.

4. The mandated reports are mere financial recordkeeping and do not compel speakers to express a viewpoint. Therefore the rules do not engage in viewpoint discrimination and warrant lesser First Amendment scrutiny.

5. The mandated reports are disclosed privately, only to the IRS and to the taxpayer, and are not made public. Therefore the dangers of compelled speech are less and the rules warrant lesser constitutional scrutiny.

In every recent case where the question has been relevant, the Supreme Court has consistently found that the disclosure of information is "pure speech" warranting the highest constitutional protections.[26] In *Bartnicki v. Vopper* the Court reasoned that "if the acts of 'disclosing' and

---

[24] *Id.*

[25] *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021).

[26] *See*, e.g. *Bartnicki v. Vopper*, 532 U.S. 514, 516 (2001)("disclosure of the contents of an illegally intercepted communication" was speech). *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 481, 115 S.Ct. 1585, 131 L.Ed.2d 532 (1995) ("information on beer labels" is speech); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759, 105 S.Ct. 2939, 86 L.Ed.2d 593 (1985) (plurality opinion) (credit report is "speech").

'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct".[27] The proposed rule, merely by mandating the disclosure of trading activity, compels brokers, so defined, to speak. As such it is a content-based and speaker-based compulsion to speak.

That said, we do not here argue that the existing broker reporting requirements as applied to customer agents or principals is unconstitutional compelled speech. The existing requirement, though never explicitly tested in the courts, *may* survive constitutional scrutiny via two different lines of First Amendment cases.

First, at the circuit level, courts have reviewed compelled disclosures of *uncontroversial factual information* that is *already in the possession of the obligated speaker* when those disclosures are made *privately to the regulator* under mere rational basis review. We will refer to these cases as *Private Facts Compulsion* cases. As we will discuss, these cases may have a limited shelf-life as recent Supreme Court precedent in adjacent case law appears to overrule substantial aspects of their holdings.

Second, a larger line of cases including cases at the Supreme Court could be used to justify compulsion under a doctrine we will call *Professional Conduct Regulation*. Both of these lines of cases will be discussed and applied to this rulemaking in turn. In both lines of cases, however, the case law can only ever justify the private disclosure of uncontroversial facts, and, as we will discuss throughout, the Treasury Department's rulemaking also compels non-traditional brokers to publicly and expressively speak viewpoints they do not wish to speak, *i.e.* the protocols and software tools that would be necessary in order to collect the information demanded in these mandated private disclosures.

Finally, after unpacking these cases and applying them to the proposed rule, we will look in turn at (A) further recent case law with respect to the First Amendment rights of data brokers and software and website developers generally, (B) older cases that offer enhanced protection for speech on matters of public concern by speakers whose motivations are not merely economic self-interest, and (C) cases where protections for speech are limited because the speech in question supports illegal activities. Ultimately there are many roads courts could take to appraise the constitutionality of the proposed rule, but each of them ultimately leads to the same destination, the rule is unconstitutional.

[27] *Bartnicki v. Vopper*, 532 U.S. 514, 516 (2001) (some internal quotation marks omitted).

Circuit level cases dealing with private facts disclosure do not support the constitutionality of this rulemaking

The D.C. Circuit in *Full Value Advisors v. SEC* found that a compelled disclosure by a regulated institutional fund manager that was made privately to the Securities Exchange Commission warranted only rational basis review.[28] The court found these compelled disclosures were constitutional:

> Here the Commission — not the public — is Full Value's only audience. The Act is an effort to regulate complex securities markets, inspire confidence in those markets, and protect proprietary information in the process. It is not a veiled attempt to "suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion."

The Eighth Circuit in *U.S. v. Sindel* found that compelled disclosures, privately to the IRS, of client information on an Internal Revenue Service form by tax attorneys were not a "compulsion to disseminate a particular political or ideological message" but sought "only to provide the government with information which his clients have given him voluntarily, not to disseminate publicly a message with which he disagrees."[29]

There are two common threads in these holdings. First, the disclosure is always made privately to the regulator, and, second, the subject matter of the disclosure is information already in the possession of the obligated party. Before applying that legal standard to the facts of this proposed rule, we must discuss whether it is even good law today. These cases are now in doubt because of recent Supreme Court holdings.

In *Bartnicki v. Vopper* the Court found that "if the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct."[30] If even the mere disclosure of uncontroversial facts or "information" is pure speech, then the rational basis scrutiny applied by the courts in *Full Value* and *Sindell* insufficiently protects the rights of speakers.

In *National Institute of Family & Life Advocates v. Becerra*, the Court overtly overruled prior opinions at the circuit level that had offered lesser constitutional scrutiny for laws regulating "professional speech," holding unequivocally that,

> [T]his Court has not recognized professional speech as a separate category of speech. Speech is not unprotected merely because it is uttered by professionals. This Court's

[28] *U.S. v. Sindel*, 53 F.3d 874 (8th Cir. 1995).
[29] *Ibid*., pg. 878.
[30] *Supra* note 23, at pg. 527.

> precedents do not permit governments to impose content-based restrictions on speech without persuasive evidence … of a long (if heretofore unrecognized) tradition to that effect.[31]

The Court clarified that there were only two narrow contexts in which professional speech garnered lesser protections, (1) the compelled disclosure of "purely factual and uncontroversial information"[32] and (2) the regulation of professional *conduct* that created a mere incidental burden on professional speech.[33]

In *Americans for Prosperity v. Bonta*, the Court made clear exactly which level of scrutiny compelled factual disclosures should trigger. The Court addressed prior ambiguity in the case law over the standard of review and summarized its recent holdings as establishing a clear standard demanding "exacting scrutiny":

> We have since settled on a standard referred to as 'exacting scrutiny.' Under that standard, there must be a substantial relation between the disclosure requirement and a sufficiently important governmental interest. To withstand this scrutiny, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights. Such scrutiny, we have held, is appropriate given the deterrent effect on the exercise of First Amendment rights that arises as an inevitable result of the government's conduct in requiring disclosure.[34]

While *Bonta* and the cases identified by the Court primarily deal with the associational rights of publicly minded groups (*e.g.* voters, civil liberties associations) whose activities may be particularly chilled by disclosure, the Court was unequivocal that the type of association bound by the law in question was not a factor in determining whether exacting scrutiny applied:

> [I]t is immaterial to the level of scrutiny whether the beliefs sought to be advanced by association pertain to political, economic, religious or cultural matters. Regardless of the type of association, compelled disclosure requirements are reviewed under exacting scrutiny. … To withstand this scrutiny, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights.[35]

As such, even if the target of the disclosure is a for-profit corporation or attorney, the standard of review should be exacting scrutiny rather than rational basis as applied by the circuits in *Full*

---

[31] *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2372 (2018)(internal quotations removed).
[32] *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2372 (2018).
[33] *Ibid*., at pg. 17.
[34] *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021).
[35] *Id*.

Value and *Sindel*. The Court in *Bonta* also clarified that this exacting scrutiny standard requires narrow tailoring, finding that:

> Narrow tailoring is crucial where First Amendment activity is chilled—even if indirectly—because First Amendment freedoms need breathing space to survive. … The government may regulate in the First Amendment area only with narrow specificity, and compelled disclosure regimes are no exception.[36]

Turning to the facts of this rulemaking, *Bonta* indicates that it is not narrowly tailored when applied to non-traditional brokers who are not customer agents or principals. The Treasury Department's proposed rule is notable for the surprising breadth of covered entities as compared with the existing definition. Rather than focusing on persons who have a discrete number of customers for whom they act as agents or principals in sales, it would classify as a broker any software developer whose published software tools or websites "provide access" to other publicly available software tools used for peer-to-peer trading of digital assets.[37] The proposed rule exempts software publishers only if the "sole function [of their software] is to permit persons to control private keys which are used for accessing digital assets on a distributed ledger."[38]

The proposed rule is also unprecedented and fails narrow tailoring due to the depth of the compelled speech obligation, the profound burden it places on those it commands to speak. As we will discuss throughout, brokers who are not customer agents or principals do not already have in their books or records the types of information the rulemaking orders them to report.[39] That information is not already "voluntarily provided" to them by their "clients" as in *Sindel*. Indeed most open source software publishers do not have customers or clients in the traditional sense at all. They merely publish tools and people, strangers to them, use those tools.[40] The proposal is not, therefore, an incidental burden on the speech activities of those it compels to report. It compels these software developers to fully rewrite their software tools to securely and rigorously collect sensitive information from their users that they otherwise have no reason or desire to collect.

---

[36] Ibid., pg. 9.
[37] *Supra* note 2.
[38] *Ibid*., at 59586. *See also*: *Ibid.*, at 59634 ("Software that provides users with direct access to trading platforms from the wallet platform is not an example of software with the sole function of providing users with the ability to control private keys to send and receive digital assets.")
[39] *Infra* pgs. 14-18.
[40] Nor is the "for compensation" requirement in conflict with this characterization, some develop tools that ultimately automatically remit a payment to the original developer. This is still not a customer relationship in any traditional sense as the user and the publisher have no contractual or agency relationship. It is more akin to an automatic payment to license or use certain intellectual properties, or an automatic payment for data transmission and publication (in this case to a public blockchain).

The private facts disclosure cases at the circuit level are, therefore, incapable of supporting the constitutionality of this rulemaking, both legally and factually. They have been overruled as to their low level of scrutiny by the Supreme Court, and they have only ever been used to justify reports of purely factual information already collected by the compelled speaker in the course of their customer-facing business. That line of reasoning does not and cannot extend to persons who are not in an agency-like relationship with the persons about whom they are compelled to make disclosures. Such a person does not have any "information which his clients have given him voluntarily";[41] indeed such a person doesn't even have clients. Moreover, the only way for such a person to collect such information would be to "disseminate publicly a message with which he disagrees,"[42] *i.e.* to develop new software that intermediates the transaction rather than software that merely enables users to make their own transactions. As in *Becerra*, that compulsion "in no way relates to the services that [targeted businesses] provide."[43] It is a compulsion made against persons who are developing software to enable non-intermediated financial transactions to speak in favor of intermediated transactions. Indeed, the rule would not merely ask these developers to voice support for alternative technologies, it would force them to build those technologies and to publish them under their name. As such, like the compulsion in *Becerra*, this proposed rule "fail[s] to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail."[44]

In another recent case, *303 Creative LLC v. Elenis*, the Court emphasized the narrow limits of constitutionality in the context of compelled disclosures of non-expressive, viewpoint-neutral facts as compared with broad constitutional prohibitions on compelling expressive and viewpoint-oriented speech:

> To be sure, our cases have held that the government may sometimes "requir[e] the dissemination of purely factual and uncontroversial information," particularly in the context of "commercial advertising." But this case involves nothing like that. Here, Colorado does not seek to impose an incidental burden on speech. It seeks to force an individual to "utter what is not in [her] mind" about a question of political and religious significance.[45]

Indeed, the policy motivation behind the speech restrictions in *303 Creative* may not be dissimilar to the motivations behind this current rulemaking. In *303 Creative*, the Court found

---

[41] *Supra* note 25.
[42] *Id.*
[43] *Supra* note 28.
[44] *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2374 (2018).
[45] *303 Creative LLC v. Elenis*, 600 U.S. ___ (2023), pg. 18.

that Colorado "intends to force [a speaker] to convey a message she does not believe with the very purpose of eliminating ideas that differ from its own."[46]

We can only speculate why the Treasury Department is brazenly going beyond the statutory authority granted them by Congress and seeking to impose recordkeeping and reporting requirements on persons who have no reason or business keeping such records. It may be that they do not want to see software in the world that enables persons to transact without an intermediary, or without a deputized agent of the state who can forcibly ensure tax reporting. Rather than seeking an outright ban on that software through legislation, this rule is instead seeking to compel Americans to only write software that enshrines an intermediary within every transaction, for that is the practical effect of this rulemaking.

Professional conduct regulation cases do not support the constitutionality of this rulemaking

The existing broker disclosure obligations as applied to customer agents and principals, though never explicitly validated in the courts, may alternatively be found constitutional as a reasonable regulation of professional conduct that incidentally burdens some speech activities of the persons engaged in that regulated conduct. In that interpretation, the conduct being regulated is that of entering into an agency relationship with a customer or else acting as the principal in a sale to the customer. While a written contract is speech, the assumption of a legal relationship that it embodies is doubtlessly conduct and can be the subject of regulation.

As the Court held in *United States v. O'Brien*, laws affecting speech that are aimed at the regulation of non-expressive conduct are still analyzed under First Amendment jurisprudence, but face a lower level of constitutional scrutiny than laws aimed directly at the regulation of expressive conduct or at speech activities themselves: "a sufficiently important governmental interest in regulating the nonspeech element [of the regulated conduct] can justify incidental limitations on First Amendment freedoms."[47] The compulsion to merely report privately to the IRS and to the taxpayer certain "purely factual and uncontroversial information" about the regulated non-expressive conduct may rightly be framed as an "incidental" limitation on traditional brokers' otherwise unabridged First Amendment rights.

The *O'Brien* standard, however, is only applicable if the rule is targeted at regulating non-expressive conduct. Things become more complicated when the rule is targeted at regulating expressive conduct or at speech itself. There is a long though underappreciated line of cases stemming from *O'Brien* that points toward a reasonably straightforward series of tests for when regulation of professional conduct that burdens speech activities is constitutional.

---

[46] *Ibid.*, pg. 20.
[47] *United States v. O'Brien*, 391 U.S. 367 (1968).

That line has been best illuminated by attorney Robert Kry in his article, "The 'Watchman for Truth': Professional Licensing and the First Amendment."[48] Kry, summarizing and synthesizing many cases, finds that

> The first question in any professional speech case should be whether the government law or regulation at issue aims at the expressive or nonexpressive component of the alleged professional's activity. Where the government action targets the nonexpressive component, actual conduct is at issue and the regulation is normally constitutional under traditional *O'Brien* principles.[49]

In the case of a broker who is, in fact, an agent of a customer or a principal in a sale to a customer, the regulation is plausibly aimed at the non-expressive component of the professional's activity. An agent under common law principles is acting on behalf of her customer. When a broker agrees to a sale, she binds the customer to that sale. The reporting requirement, therefore, is merely a requirement to disclose certain facts about one's sales, *i.e.* one's conduct as an agent. As a principal in a sale to a customer, the broker is, once again, engaged in conduct, a sale, and the reporting requirement merely discloses facts about that conduct. Additionally, brokers of this type are in most cases already subject to a licensing or registration requirement under other statutes.[50] Those forms of professional conduct are traditionally regulated and the tax laws merely provide for an additional recordkeeping and reporting requirement associated with that conduct. Altogether, the reporting requirement, though compelled speech, appears to be a regulation aimed at the non-expressive component of a professional's activity. It is therefore likely constitutional.

As described earlier however, the Treasury Department's proposed rule inappropriately departs from that customer agent or principal standard and seeks to compel speech from persons who are engaged in no such regulated conduct. A mere publisher or maintainer of software, websites, or smart contracts is not in an agency relationship with any customer, nor is she selling anything to any customer apart from, potentially, a license to use her tools or a fee charged for relaying or publishing the user's data on a communications network or blockchain. Additionally, unlike typical brokerage, these activities do not trigger any licensing or registration requirements under other state or federal statutory schemes.

Indeed, even when such person is relaying actual cryptocurrency transaction messages that, once recorded in the blockchain, will effect a sale of some cryptocurrency, these entities

---

[48] *Id.*

[49] Robert Kry, "The 'Watchman for Truth': Professional Licensing and the First Amendment," 23 *SEATTLE U. L. REV.* 885 (2000).

[50] For example under the Securities Exchange Act of 1934, codified at 15 U.S.C. § 78a et seq. or the Investment Advisers Act of 1940, codified at 15 U.S.C. § 80b-1 through 15 U.S.C. § 80b-21.

typically have no actual ability to act on behalf of the user and no actual or apparent authority under agency law to act on their behalf. At most, they can choose whether or not to relay the signed transaction message (but so too can an internet service provider); they cannot alter the contents of that message such that the terms of the sale would change. They cannot and do not act as an agent of any customer nor are they a principal in a digital asset sale to any customer.[51]

These persons may be involved in conduct in other ways, such as paying for web hosting services, paying fees on cryptocurrency networks to record software or data in the blockchain, taking fees from users to relay their messages, or simply paying rent or otherwise maintaining facilities wherein they or their employees do the work of developing software or maintaining communications tools, but all of those activities are aimed at engaging in speech, the publication of software and data, and none of those activities give rise to the type of fiduciary or agency-like financial relationship, *i.e.* conduct, that justifies third-party tax reporting obligations.

Moreover, these persons have deliberately designed their software, websites, and smart contract tooling such that it can be useful to a trader and capable of facilitating their trades or other desires *without* the need for any agency relationship or for any legal or trust-based relationship with the publisher or any other party whatsoever. The user can and does do it all themselves. That is the point of cryptocurrency and "decentralized finance." We can debate the merit of such a design goal,[52] but what is not debatable is that this is how these tools are presently designed.[53] By demanding that these publishers rewrite their tools such that an agency relationship is established between the author of the tool and its user, such that the name,

---

[51] As we wrote earlier, we do not object to applying the existing customer agent or principal standard in the context of digital asset middleman. Therefore, should any entity in the cryptocurrency ecosystem be found to have actual or apparent authority (under any statutory common law agency standards) to act on behalf of another person in a sale of cryptocurrency, then broker reporting obligations should apply.

[52] A reasonable concern with that goal is that the disintermediation of financial services results in the loss of centralized chokepoints that have been economically efficient targets for engaging in financial crime surveillance or otherwise achieving public policy goals such as investor protection. The mere fact that many in government may have these concerns, however, does not somehow make speech that embodies these, to-some, questionable goals less protected as speech. *See*: *Supra* note 42, at pg. 3 ("The First Amendment protects an individual's right to speak his mind regardless of whether the government considers his speech sensible and well intentioned or deeply misguided, and likely to cause anguish or incalculable grief.").

[53] Jerry Brito, "The Case for Electronic Cash," *Coin Center Report*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/; Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center Repor*t, March 2019, https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/ (*in pgs. 55-69; Appendix: Building Electronic Cash and Decentralized Exchange Software*); *See also*: "MetaMask Documentation: Architecture," accessed November 1, 2023, https://docs.metamask.io/wallet/concepts/architecture/.

Social Security number, and other intimate details of the user are entrusted to the alleged "broker," the regulation is squarely aimed at compelling not merely the disclosure of trading data and taxable gains, but also the compelled creation of significant expressive software and tooling to solicit and collect data in a manner that would otherwise be antithetical to the goals of the software developer. Such an order is so unprecedented that it is difficult to find appropriate metaphors or past examples. It is as if a state—frustrated that it cannot determine who is reading which books—ordered that novelists shall hold in-person book readings during which they must collect and report information about their audience.

Accordingly, when applied to mere publishers and maintainers of software, websites, and smart contracts, these regulations target the expressive activity of the alleged broker. That does not mean, however, that such rules will automatically be unconstitutional. The Court has dealt with several regulatory schemes aimed at expressive professional conduct, such as a lawyer giving legal advice to a client. Throughout these cases the Court has developed a robust series of standards for constitutionality that are focused primarily on "which kinds of advice are licensable based on how closely they resemble forms of communication associated with fiduciary relationships."[54] This leads us to the second question in Kry's analysis of the First Amendment limits to regulating professional conduct, what he calls the "value neutral test" because it applies irrespective of whether the speech affected is a matter of public concern and irrespective of the motives of the speaker:

> If the regulation aims at the expressive component of the activity, a court should analyze it under the value-neutral test. Two questions need to be addressed: (1) Is the speech characteristic-dependent, in that the substance of the advisor's message depends on the recipient's circumstances? (2) Is the speech delivered in the context of a person-to-person relationship, one in which the professional is communicating to a single person with whom he is directly acquainted? Unless both of these questions can be answered in the affirmative, the government licensing scheme is impermissible.[55]

Given the in-person and client-specific nature of legal services, there should be no surprise that under these cases the professional regulation of attorneys, including licensing, limits on solicitation and advertising, and—as in this rulemaking—compelled disclosures, typically withstands constitutional scrutiny. In the context of developers of cryptocurrency systems, however, the answer to Kry's twin questions of *characteristic-dependence* and *person-to-person context* is an unqualified "no." It is taken as written that software, websites, and smart contracts in the cryptocurrency space are built such that they are generic, serving the needs of whoever wants to use them irrespective of the characteristics of that user. It is also a given that these

[54] *Supra* note 46.
[55] *Ibid*.

tools are shared widely over the internet and used freely by whoever happens to download them or (in some cases) whoever pays to license the software or pays to have their transactions relayed by the software. As such, they are never "delivered in the context of a person- to-person relationship."[56] Accordingly, regulation of the speech activities of these developers, including compulsions to report and develop expressive software that enables that reporting, would face strict scrutiny by the Court and be found unconstitutional.

While these standards are general principles that are equally applicable to any kind of expressive conduct regulation, it is nonetheless worth noting that several of the cases that first articulated these standards dealt explicitly with speech, including software, that advised and facilitated sales of valuable assets. As such, the speech in question in these cases was *very similar factually* to the speech that would be burdened under the Treasury Department's proposed rule. The value-neutral test was developed in *Lowe v. SEC*, a case involving the unconstitutional application of the Investment Advisers Act to a person merely publishing a public newsletter,[57] and it was further reinforced in *Taucher v. Born*[58] and two similar cases[59] dealing with the unconstitutional application of the Commodities Exchange Act to the developers of commodities trading software.[60]

The Court's recent cases offer even stricter First Amendment protections for data brokers and web developers

Kry's 2000 article was ahead of its time and in the intervening years the Court has trended even further toward protecting speech activities in the context of professional conduct regulation. In *IMS Health v. Sorrell*, the Supreme Court found that a ban on the sale of prescriber identifying information by-and-to marketing professionals and data brokers was an unconstitutional speaker- and content-based burden on protected expression.[61] The Court found that it was unnecessary to determine whether the data being bought and sold was protected speech or merely a valuable commodity, it was enough that the law burdened the expressive activities of marketers and data brokers. The Court reasoned that the law in question:

> [C]ould be compared with a law prohibiting trade magazines from purchasing or using ink. Cf. Minneapolis Star. Like that hypothetical law, [the law in question] imposes a speaker- and content-based burden on protected expression, and that circumstance is sufficient to justify application of heightened scrutiny. As a consequence, this case can

[56] *Lowe v. SEC*, 472 U.S. 181, 185 (1985).
[57] *Supra* note 58.
[58] *Taucher v. Born*, 53 F. Supp. 2d 464, 476-78 (D.D.C. 1999);
[59] *Accountant's Soc'y of Va. v. Bowman*, 860 F.2d 602, 603-05 (4th Cir. 1988); *Commodity Trend Serv., Inc. v. Commodity Futures Trading Comm'n*, 149 F.3d 679 (7th Cir. 1998).
[60] *Ibid*.
[61] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 583 (2011).

> be resolved even assuming, as the State argues, that prescriber-identifying information is a mere commodity.[62]

Indeed, even if the expanded broker definition contemplated in this rulemaking was incorrectly found to be regulating merely the non-expressive conduct of persons engaged in the publication of software, websites, or data, it would still face heightened scrutiny and be found unconstitutional under the test outlined in *Sorrell*, as a speaker- and content-based burden on protected expression.

The Court has also recently held that these highly speech-protective standards apply at least as strongly in the context of publishing and maintaining software and websites online as they do in the more traditional context of offline professions. Indeed, in *303 Creative*, the Court articulated a much more protective standard for web developer speech.

The Court held that it would be unconstitutional "to forc[e a web developer] to create custom websites."[63] Indeed, rather than analyzing the compelled speech in that case under the professional conduct standards discussed above, the Court found that the act of publishing websites containing "images, words, symbols, and other modes of expression" was protected as "pure speech" and not as expressive conduct.[64] The Court explicitly rejected the premise, argued by the government, that the regulation was focused merely on selling web development services (*i.e.* on regulatable conduct). The Court did not care whether the speech in question was characteristic-dependent or delivered in-person (and it probably was both of those things). Indeed, without any discussion of the reasonable limits of professional regulation of web developers, the Court held that obligating a web developer to design websites celebrating marriages that she does not wish to celebrate simply and unconstitutionally compelled her to speak viewpoints with which she disagreed.

The Treasury Department's proposed expansion of the reporting rule forces web developers to design websites that collect information that the developer does not, for deeply held political and ideological reasons, wish to collect. In addition to failing the looser constitutional standards for professional regulation discussed in the previous section, the proposed rule is an exact match for the highly protective constitutional standard articulated in *303 Creative*, and therefore unconstitutional.

---

[62] *Id.*, at 2.
[63] *Supra* note 45, at 3.
[64] *Id.*, at 9.

The regulation unconstitutionally compels speech even under older case law with less-protective standards.

Kry's article goes on to outline a third and final step in the analysis applicable only if the earlier steps so far failed to find the professional regulation unconstitutional. These tests are based on a series of older First Amendment cases dealing primarily with what might be loosely called "high-value speech," speech on matters of fundamental political or social importance spoken by persons with motives beyond mere self-enrichment, *e.g.* non-profit organizations and labor unions. We believe that even under Kry's less-protective 'value-neutral' standard, the expansion of the broker definition contemplated by the Treasury Department in this rulemaking is unconstitutional. For completeness, however, we will nonetheless discuss Kry's value-based test as well:

> Finally, even if a regulation is valid under the value-neutral test, a court should apply the value-based test. The court should examine whether the professional's speech involves a matter of public concern.
>
> The court should also consider whether the speaker is motivated at least in part by interests other than self-enrichment. If both of these conditions are met, the government restriction is invalid.[65]

Cryptocurrency tooling and data, whether protocol software, so-called decentralized finance applications and smart contracts, or the relayed transaction messages and blockchains themselves are, without question, matters of public concern. Contrasted with proprietary trading algorithms or the secret individual buy and sell orders of a particular trader at an over-the-counter desk, these technologies are intended to be public, as in generally revealed for the public to see, as well as public, as in an alternative financial instructure developed as a public good for all to use. These tools are intended to build and support an alternative financial system that would embody certain deeply held political and social goals of their developers, such as individual privacy and agency over one's own financial dealings.[66] Unmistakably, many in the cryptocurrency space are also motivated by the prospect of self-enrichment. However, it would be a gross misstatement to suggest that earnest cryptocurrency developers who have built their tools to avoid the need for trust between user and developer (those who we argue should be exempted from this rulemaking) are in it for self-enrichment alone; there are much easier ways to get rich than building a trust-minimized alternative to the global financial system.

---

[65] *Supra* note 48.
[66] Jerry Brito, "The Case for Electronic Cash," *Coin Center Report*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/.

Regardless, in the years since Kry's article the Court has further collapsed the distinction between commercial and non-commercial speech such that so-called "low value speech" (*e.g.* commercial speech or profit-motivated speech) is no longer treated differently. The Court has clarified that corporate speech is entitled to no less protection as speech by individuals,[67]and therefore that professional speech is entitled to no less protection than speech outside of the professional context.[68] And, as we saw in the *Sorrell* opinion, even corporate expressive conduct—the buying and selling of prescriber-identifying information, undertaken for profit-oriented purposes, targeted marketing of non-generic prescription drugs to doctors—is entitled to strict First Amendment protection.

That said, even if the Court was to turn its back on this trend of enhanced protections for profit-motivated speech on matters merely of private concern, this regulation would remain unconstitutional under the older value-based standards cataloged by Kry: it burdens speech that is fundamentally on a matter of public concern (the scientific and technical methods and mechanisms for creating a financial system that enables greater individual freedom and privacy) and it burdens speakers who are motivated, at least in part, by interests other than self-enrichment (the desire to see that new and better financial system made available to all).

The regulation cannot be defended as a reasonable prophylactic against lawbreaking.

Aspects of the professional conduct cases discussed above could be used to articulate a special rule in the context of cryptocurrency tools that might, wrongly, justify regulations that burden speech. In essence it could be argued that these speech activities are largely unprotected because compelled disclosures are needed as a prophylactic against subsequent illegal activity that may otherwise be facilitated by the speech.

In the narrow context of attorney in-person solicitation, speech that is "inherently conducive to … forms of misconduct" has received lesser First Amendment protections.[69] As discussed in the sections above, cryptocurrency software, websites, and smart-contracts, unlike in-person legal advice, are published as generic tools, rather than being tailored to the needs of an individual recipient, and they are published to the public at large over the internet rather than being delivered in-person. Accordingly, this case law is already ill-suited to buttressing this proposed rule.

[67] "Nor, this Court has held, do speakers shed their First Amendment protections by employing the corporate form to disseminate their speech." *303 Creative LLC v. Elenis*, No. 21-476, at *23 (June 30, 2023).
[68] *Supra* note 41.
[69] *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447 (1978), at 464.

Nonetheless, the policy reasoning for restricting in-person attorney solicitation mirrors some of the reasoning for an expansive broker rule. For example, in *Ohralik v. Ohio State Bar Assn.*, the Court articulated the danger it perceived from allowing in-person attorney solicitation:

> The aim and effect of in-person solicitation may be to provide a one-sided presentation and to encourage speedy and perhaps uninformed decisionmaking; there is no opportunity for intervention or counter-education by agencies of the Bar, supervisory authorities, or persons close to the solicited individual.[70]

One could attempt to argue that because of the speed and ease by which a user of cryptocurrency tools can commit to financial transactions and because of the lack of a regulated party in the loop, the publication of these tools somehow warrants less protection given the inherent dangers they present. The Court in *Oharlik* supported the constitutionality of restrictions on in-person solicitation by citing *Chaplinsky v. New Hampshire*, the paradigmatic "fighting words" case, which held that states may punish those words "which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[71] The Court emphasized the "immediacy of a particular communication and the imminence of harm" as "factors that have made certain communications less protected than others."[72]

Applying this line of reasoning to restrictions on the publication of cryptocurrency software and tools may be attractive to some who wrongly and prejudicially believe that cryptocurrency is useful only to criminals and possesses literally no redeeming technical, social, or political value. These advocates, however, would be wrong on the facts and the law.[73] Factually, it is plainly true that many, indeed most, cryptocurrency users are not engaged in any crimes.[74] Indeed, many are patriotic Americans who see embodied in these technologies the same principles of individual liberty and equality under the law that informed the founding.[75] Legally, only a very narrow set of speech has ever been found to be so prone toward the incitement of *truly imminent* and *specific* lawless action as to warrant lesser protection. Even speech that

---

[70] *Id.* at 457.
[71] *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942), at 572.
[72] *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447, 457 (1978) ("Unlike a public advertisement, which simply provides information and leaves the recipient free to act upon it or not, in-person solicitation may exert pressure and often demands an immediate response, without providing an opportunity for comparison or reflection.")
[73] Andrea O'Sullivan, "What is cryptocurrency good for?" *Coin Center Explainer*, July 30, 2018, https://www.coincenter.org/education/blockchain-101/what-is-cryptocurrency-good-for/.
[74] *See* generally, the annual reports from industry-leading blockchain analytics firm, Chainalysis. https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/ (finding that the share of illicit activity across all cryptocurrency transactions was less than 1 percent).
[75] Jerry Brito, "The Case for Electronic Cash," *Coin Center Report*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/

advocates only *generally* for the violent overthrow of the government at some *indeterminate future time* remains fully protected.[76]

While it is true that some small minority of persons may use cryptocurrency tools for crime it is patently absurd to suggest that the mere publication of these tools tends to incite any imminent wrongdoing. If the standard was *mere propensity that some in the audience will commit crimes and that these criminals may be marginally more successful in their criminal undertakings because of their hearing the speech*, then little speech would ever garner constitutional protections.

The IRS is free to—and indeed should—investigate any efforts by software developers or others to *knowingly* and *intentionally* promote *imminent and specific acts* of money laundering and tax evasion. Speech that is directly in furtherance of a crime garners no protections. However, any crime-preventing prophylactic regulation of speech must still be narrowly tailored to address actual wrongdoing and it must not substantially burden speech that is protected and unrelated to the criminal activities to be prevented. Therefore, the government should not and cannot constitutionally criminalize an entire range of software publishing simply because some minority fraction of the users of that software will use it to hide their wealth or criminal proceeds.

Again, these tools can be used by anyone for any purpose and the vast majority of usage is not criminal or in any way illicit.[77] Moreover, the end goal of many of the publishers of these tools is merely to provide tools and technologies that enable people to handle their own money without relying on intermediaries. Ordinary people want control over their assets just as much as criminals do. The publishers of these tools are motivated by a fear that the financial system has become noncompetitive, predatory, and exploitative of its users. They want people to be able to transact and manage their assets on their own, as was once possible and indeed common when day-to-day transactions were made primarily using cash, coins, and other tangible financial instruments. That general goal of financial independence is not an inappropriate goal merely

---

[76] *Brandenburg v. Ohio*, 395 U.S. 444, 448 (1969) ("Ohio's Criminal Syndicalism Act cannot be sustained. The Act punishes persons who advocate or teach the duty, necessity, or propriety of violence as a means of accomplishing industrial or political reform; or who publish or circulate or display any book or paper containing such advocacy; or who justify the commission of violent acts with intent to exemplify, spread or advocate the propriety of the doctrines of criminal syndicalism; or who voluntarily assemble with a group formed to teach or advocate the doctrines of criminal syndicalism. ... Accordingly, we are here confronted with a statute which, by its own words and as applied, purports to punish mere advocacy and to forbid, on pain of criminal punishment, assembly with others merely to advocate the described type of action. Such a statute falls within the condemnation of the First and Fourteenth Amendments.")

[77] "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking," *Chainalysis*, January 12 2023, https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/.

because a minority of people will abuse that independence in order to violate the law, and we should not wish for Americans to remain utterly reliant on a for-profit banking and payment system merely because the alternative, self-reliance, might allow some Americans to commit crimes.

Ultimately any attempt to extend the holding in *Ohralik* to cryptocurrnecy would encounter at least the same difficulty as a proposed extension of in-person solicitation bans did in a subsequent case, *Edenfield v. Fane*:

> Were we to read *Ohralik* in the manner ... propose[d], the protection afforded commercial speech would be reduced almost to nothing; comprehensive bans on certain categories of commercial speech would be permitted as a matter of course. That would be inconsistent with the results reached in a number of our prior cases. ... It would also be inconsistent with this Court's general approach to the use of preventative rules in the First Amendment context. "Broad prophylactic rules in the area of free expression are suspect. Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms."[78]

The proposed broker regulations are not precise; they wrongly extend information collection and reporting obligations to persons who have no extant ability or inclination to gather the relevant information. They force software developers to alter their tools so substantially that they would effectively change their professions from mere publishers of tools that allow persons to transact freely into gatekeepers who lock their tools and capabilities away from anyone unwilling to identify themselves and submit to a fully intermediated surveillance regime. Irrespective of the efficacy of any potential prophylactic such overbroad speech regulation might provide against crime, the regulation is squarely against the fundamental rights of Americans to speak and be free from compelled speech.

The proposed rule violates the Fourth Amendment rights of persons writing, maintaining, and using the software and services of "brokers" who are neither customer agents nor principals

In two significant cases from the 1970s, the Court held that neither bankers nor bank customers had a reasonable expectation of privacy over bank records.[79] These cases rejected challenges to the constitutionality of the Bank Secrecy Act, a law that requires financial institutions to keep and report records about their customers to the Treasury Department without a warrant.[80]

---

[78] *Edenfield v. Fane* 507 U.S. 761 (1993)(Citing NAACP v. Button).
[79] *California Bankers Assn. v. Shultz*, 416 U.S. 21, (1974) and *United States v. Miller*, 425 U.S. 435 (1976).
[80] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-4 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.).

These cases also formed the basis of what would become known as the third party doctrine, a carve-out from Fourth Amendment protections against warrantless searches for narrow categories of information voluntarily provided by the target of the search to a third party for a legitimate business purpose.[81] Recently, the Court has expressed serious doubt over the continued application of the third party doctrine in the context of modern technologies that, by and large, direct people to perform all of their day-to-day activities via third parties (*e.g.* email providers, social networks, video conferences, and electronic payments systems) leaving almost none of the digital equivalents to what were once personal papers and effects protected from warrantless search and seizure.[82]

The constitutionality of the proposed broker reporting regime hangs on our discussion of compelled speech in the previous section, but it also hangs on the rule *only* mandating the collection of information over which neither the target of the compulsion (the broker) nor the subject of the record (the customer) have any reasonable expectation of privacy. We will begin with a look at the existing case law up to the recent *Carpenter* case that puts the third party doctrine in doubt. In this pre-*Carpenter* context, we find that the extension of reporting obligations is inappropriate even under the permissive standards of the original third party doctrine. Within this section we will look at both the Fourth Amendment interest of the obligated entity, the broker, and then the interest of the users of the broker's tools. In both cases we find that existing case law does not support the constitutionality of the proposal. We will then turn to the *Carpenter* case and other recent case law that suggests an even steeper uphill climb for the government to justify the warrantless collection of data from persons who are not brokers in the traditional sense, *i.e.* are not customer agents or principals in sales.

Privacy interest of the "broker"

The basis for allowing warrantless searches of a bank's or other financial intermediary's records is the administrative search doctrine, sometimes referred to as the business records exemption. The touchstone of any Fourth Amendment search is reasonableness.[83] In most contexts reasonableness requires a warrant particularly describing the person and places to be searched or seized and probable cause for the issue of that warrant as judged by a neutral magistrate. In a handful of specific contexts, the Court has found that certain searches can be reasonable even in the absence of a particular warrant, probable cause, or a neutral magistrate. Searches of business records by administrative agencies to ensure compliance with regulations are sometimes one of these special categories of reasonable warrantless search. The existing broker reporting rule may withstand Fourth Amendment challenges based on this line of cases. Most

[81] *See, generally* Orin S. Kerr, "The Case for the Third-Party Doctrine," 107 MICH. L. REV. 561 (2009).
[82] *Id.* at 597.
[83] *Camara v. Municipal Court*, 387 U.S. 523, 539 (1967) ("reasonableness is still the ultimate standard.")

cited is *United States v. Morton Salt Co*. The Court in *Morton* refused to answer the question of whether a business and its records are protected under the Fourth Amendment but found that,

> [N]either incorporated nor unincorporated associations can plead an unqualified right to conduct their affairs in secret. … While they may and should have protection from unlawful demands made in the name of public investigation, corporations can claim no equality with individuals in the enjoyment of a right to privacy.[84]

The Court held that businesses should be free from unlawful intrusions into their records by the state but stopped short of calling for a warrant, probable cause, or a neutral magistrate. Instead the Court suggested a flexible standard for reasonableness in the case of administrative searches:

> It is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.[85]

As we argued in the first section, the collection of records from persons who are not customer agents or principals is not "within the authority of the agency." We will not rehash that argument here but believe this alone is deadly to the Fourth Amendment constitutionality of the proposed rule.

As we argued in the second section, the records sought do not yet exist within the records of the alleged brokers, none of these entities have any reason to collect the requested information and none currently do so. In this sense, under *Morton*, the demand may not be "reasonably relevant" although the *Morton* holding is unclear whether that "relevance" relates to the nature of the business being searched or the nature of the regulatory scheme being policed. While it may be arguably reasonable for a dentist to be compelled to keep dental x-rays on file so that police can identify homicide victims, surely it would be unreasonable for the state to compel dentists to also collect and record their patients' fingerprints. A database of fingerprints would certainly be *relevant* to catching murderers but it would certainly not be *relevant* to the practice of dentistry.

The Court in *Morton* calls for diminished corporate privacy rights due to the nature of businesses as compared with individuals, so-called, artificial vs. natural persons: "They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities. The Federal Government allows them the

[84] *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), at 652.
[85] *United States v. Morton Salt Co*., supra, at 652-653.

privilege of engaging in interstate commerce. Favors from the government often carry with them an enhanced measure of regulation."[86]

This reasoning too cannot be applied to defend the proposed rulemaking. The proposed definition of "broker" as it applies to persons who are not customer agents or principals contemplates extending warrantless records searches and seizures to individuals who design software qua individuals. A significant number of cryptocurrency and decentralized exchange projects are developed by groups of otherwise unaffiliated software developers. Moreover, even those who work within incorporated entities engage primarily in protected speech activities. Rather than having "the privilege of engaging in interstate commerce" these persons are exercising the right to buy and sell within "a free marketplace of ideas, a marketplace that provides access to social, political, esthetic, moral, and other ideas and experiences."[87]

This distinction between burdening the mere business activities of the target of an administrative search and the fundamental rights of that target would ultimately be key to the constitutionality of warrantless searches of bank customer records in *California Bankers Association v. Shultz*.

In *California Bankers* the Court validated the constitutionality of the Bank Secrecy Act, citing *Morton*.[88] The Banks argued that they were being made to collect information on activities outside the scope of their business, information about transactions for which they were mere bystanders.[89] The Court suggested this characterization was entirely inappropriate, that the information collected was about the Bank's actual business conduct itself, conduct that benefited the bank immensely and that relied upon a body of law and regulation for its profitability. Thus the "favor" from the government that warranted a warrantless intrusion into their records. The Court reasoned:

> The bank plaintiffs proceed from the premise that they are complete bystanders with respect to transactions involving drawers and drawees of their negotiable instruments. But such is hardly the case. A voluminous body of law has grown up defining the rights of the drawer, the payee, and the drawee bank with respect to various kinds of negotiable instruments. The recognition of such rights, both in the various States of this country and in other countries, is itself a part of the reason why the banking business has flourished and played so prominent a part in commercial transactions. The bank is a party to any negotiable instrument drawn upon it by a depositor, and upon acceptance or payment of an instrument incurs obligations to the payee. While it obviously is not

[86] *Id.*
[87] *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011) at 583.
[88] *California Bankers Assn. v. Shultz*, 416 U.S. 21 (1974) at 66-67.
[89] *Id.*

> privy to the background of a transaction in which a negotiable instrument is used, the existing wide acceptance and availability of negotiable instruments is of inestimable benefit to the banking industry as well as to commerce in general.
>
> Banks are therefore not conscripted neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance. Congress not illogically decided that if records of transactions of negotiable instruments were to be kept and maintained, in order to be available as evidence under customary legal process if the occasion warranted, the bank was the most easily identifiable party to the instrument and therefore should do the recordkeeping.[90]

Unlike banks, the developers and publishers of cryptocurrency software, websites, and smart contracts are not parties to the transactions users of their software or tools may make. A Bitcoin or Ethereum transaction message, once signed by the individual sender and incorporated into the blockchain, is a valid final transfer of digital assets. It is not a negotiable instrument, it is not a debt owed by any party, it is not a contract (despite the unfortunate informal term "smart contract"), it is not even a bearer instrument. A person pays another person in these networks by changing a record on the blockchain. Once that record changes, the recipient should be satisfied that the transfer has occurred. She does not need to take the signed transaction message to some non-existent Bank of Bitcoin that will be obliged under the law to redeem the instrument for bitcoins. The fact that the record exists means she has been paid.[91] Accordingly, unlike other financial or legal instruments, there are no laws or government guarantees that backstop the value of the transaction. Therefore, unlike banks, developers do not have a "substantial stake" in some government-facilitated "continued availability or acceptance" of cryptocurrency transactions. There is no such government favor being given to developers in a bargain to allow reasonable warrantless surveillance.

There are, of course, some persons in the cryptocurrency space who *are* operating businesses wherein the customer-business relationship is, in fact, mediated and backstopped by law and regulation rather than the guarantees of software and protocols. These are the "hosted wallet" providers of the contemplated rulemaking. They obligate themselves legally to hold cryptocurrencies on behalf of their customers and their customers pay them for the convenience. This category also includes persons, like investment advisors, dealers, and fund managers, who affirmatively promise to act in the best interests of their clients and who have actual or apparent authority to do so irrespective of their custody over customer funds. We do

---

[90] *Id.* at 48.

[91] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 31, 2008, https://bitcoin.org/bitcoin.pdf.

not argue that such persons should also be excluded from regulation or the reporting obligations of the proposed broker rule. Indeed we argue the opposite, that reporting obligations are reasonable as applied to persons in a customer agent or principal relationship. However, if the target of the reporting obligation is merely providing a "facilitative service" in the form of a public website, software, or access to smart contracts, and has no such agency relationship with their users, the obligations are not reasonable. Unlike the banks in *California Bankers*, these persons are conscripted neutrals in the transactions they would be forced to report on. Accordingly, these searches are not reasonable even under the lower privacy guarantees afforded targets of administrative searches.

Another line of Fourth Amendment cases justifies warrantless administrative searches of businesses that are "pervasively regulated." These cases argue that persons who choose to enter certain lines of business that are well-known to be "pervasively regulated," are assuming the risk of warrantless intrusions and, accordingly, their reasonable expectations of privacy are diminished.[92] It just comes with the territory, suggests the Court. Although the Court in *California Bankers* cited these cases in its rationale for why bankers have lesser privacy over their records, banking is not included in the Court's own short list of pervasively regulated businesses. In the 2015 case *City of L.A. v. Patel*, the Court refused to add the hotel industry to the list of pervasively regulated businesses and, accordingly, invalidated a law that forced hotels to keep and disclose lists of their guests to the police without a neutral magistrate preventing abusive searches. The Court reasoned that the bar for "pervasively regulated" was very high:

> Over the past 45 years, the Court has identified only four industries that "have such a history of government oversight that no reasonable expectation of privacy . . . could exist for a proprietor over the stock of such an enterprise."[93]

Those four industries are liquor sales, firearms trade, mining, and automobile junkyards. Banking should probably be on that list as well as *United State v. Biswell* (a case that validated warrantless inspections of gun dealerships) was cited repeatedly for the proposition that bankers should have diminished privacy expectations over their own records. The Court in *Biswell* offers a much deeper look at why the mere pervasiveness of regulations should affect the privacy expectations of persons engaged in certain industries:

> It is also plain that inspections for compliance with the Gun Control Act pose only limited threats to the dealer's justifiable expectations of privacy. When a dealer chooses

[92] In cases dealing with liquor sales, *Colonnade Catering Corp. v. United States*, 397 U.S. 72 (1970), firearms dealing, *United States v. Biswell*, 406 U.S. 311, 311–312 (1972), mining, *Donovan v. Dewey*, 452 U.S. 594 (1981), and running an automobile junkyard, *New York v. Burger*, 482 U.S. 691 (1987).
[93] *City of L. A. v. Patel*, 576 U.S. 409, 424 (2015).

> to engage in this pervasively regulated business and to accept a federal license, he does so with the knowledge that his business records, firearms, and ammunition will be subject to effective inspection. Each licensee is annually furnished with a revised compilation of ordinances that describe his obligations and define the inspector's authority. 18 U.S.C. § 921 (a) (19). The dealer is not left to wonder about the purposes of the inspector or the limits of his task.[94]

Unlike gun dealers, software developers and other mere communications intermediaries are not subject to some hypothetical Communications Control Act. Indeed, such an act would almost certainly be unconstitutional on First Amendment grounds. These persons have entered an industry where the assumption is that, far from being regulated, their day to day activities will, in fact, be protected from unreasonable government interference. The few developers to find themselves on the wrong end of censorship orders have, in fact, successfully sued their would-be regulators and been repeatedly vindicated.[95] To argue that a developer of software, websites, or smart-contracts "is not left to wonder about the purposes of the inspector or the limits of his task" is absurd because there are no regulatory schemes that yet create and empower such inspectors, indeed the constitution broadly forbids it.

Finally, the Court in *Biswell* also emphasized the limited "possibilities of abuse and the threat to privacy" inherent in allowing inspectors to conduct occasional in-person inspections of a gun dealer's premises without a warrant. The Court, perhaps playfully, spelled out that the "seizure of respondent's sawed-off rifles was not unreasonable under the Fourth Amendment."[96] In the context of the proposed broker reporting rule expansion, the risk-reward calculus of warrantless searches is not so unbalanced. The reports demanded by the proposed broker rule are not occasional in-person inspections of a handful of retail establishments; they demand the recurring automatic reporting of thousands and even hundreds of thousands of individual persons' full transaction history in digital assets. While it is true that these tools are not yet "mainstream" in that they are not yet involved in an ordinary American's purchase of daily essentials, it is very possible that they will one day be mainstream and pervasive. If only for that mere possibility, the Court would be well-advised to protect such a detailed and intimate record of ordinary Americans' economic life from one day being the casual object of mass warrantless surveillance. As Justice Joseph Bradley, writing for the Court, said long ago in *Boyd v. United States*,

---

[94] *United States v. Biswell*, 406 U.S. 311, 311–312 (1972)
[95] *See generally,* Alison Dame-Boyle, "EFF at 25: Remembering the Case that Established Code as Speech," *Electronic Frontier Foundation*, April 16, 2015, https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech.
[96] *United States v. Biswell*, 406 U.S. 311, 311–312 (1972).

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.[97]

In summary, it is therefore arguably constitutional under the administrative search doctrine to require records and reports without warrants from typical bankers, brokers, and arms dealers, but it is not at all appropriate to do so of software developers and other mere communications intermediaries.

Privacy interest of the users pre-*Carpenter*

Plaintiffs in *California Bankers* also argued that the reporting requirements violated the Fourth Amendment rights of bank customers, but the Court found that no plaintiff could bring such a claim. The bankers association could not claim to represent the rights of customers harmed by the reporting requirement,[98] and the ACLU, while it did have accounts with BSA-regulated banks, had not engaged in any currency transactions over $10,000, and therefore would never have been the subject of a CTR report.[99] No harm no foul. These claims would have to wait for the next case, *US v. Miller*, to be tested.

However, in separating the analysis between the seizure of records, which was discussed in *California Bankers*, and the search, which would have to wait for *Miller*, the Court may have prejudged the outcome. As Justice Marshall, in a scathing dissent from the *California Bankers* majority, wrote:

> The seizure has already occurred, and all that remains is the transfer of the documents from the agent forced by the Government to accomplish the seizure to the Government itself. Indeed, it is ironic that, although the majority deems the bank customers' Fourth Amendment claims premature, it also intimates that, once the bank has made copies of a customer's checks, the customer no longer has standing to invoke his Fourth Amendment rights when a demand is made on the bank by the Government for the records. By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow

[97] 116 U.S. 616 (1886).
[98] *Id*. 59-70.
[99] *Ibid*.

> charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late.[100]

Justice Marshall's concern proved prescient. In *Miller*, the respondent had been indicted, effectively, for conspiracy to make moonshine, and the evidence at stake in the indictment was a series of transactions he had made through his bank for cargo van rentals, radio equipment, and metal piping.[101] The bank had records of these transactions that it retained as per the implementing regulations of the BSA, and, when subpoenaed by the Treasury Department's Alcohol, Tobacco and Firearms Bureau, the bank turned these records over to investigators.[102]

Again, the Court held that Miller had no reasonable expectation of privacy over these records because he had knowingly revealed this information to the bank during the usual course of business; the records were as much the bank's information as Miller's, and the bank was free to share them with law enforcement through the usual, warrantless legal processes:

> The checks are not confidential communications, but negotiable instruments to be used in commercial transactions. All of the documents obtained, 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.[103]

The Court refused to entertain Miller's arguments that it was the combined compulsion of the bank by the government to collect the information in the first place and the subsequent subpoena of that information once collected that constituted a search and seizure. Instead it merely analyzed, separately, whether Miller had a reasonable privacy expectation over the copies of the checks (no, because they are business records) or the original checks that were copied (no, because they were willingly handed over to a third party).[104]

Again, Justice Marshall lambasted the bifurcated analysis as a sham:

> Today, not surprisingly, the Court finds respondent's claims to be made too late. Since the Court in [*Shultz*] held that a bank, in complying with the requirement that it keep copies of the checks written by its customers, "neither searches nor seizes records in which the depositor has a Fourth Amendment right," [] there is nothing new in today's holding that respondent has no protected Fourth Amendment interest in such records.

---

[100] *Id*. 97.
[101] *United States v. Miller*, 425 U.S. 435 (1976) https://supreme.justia.com/cases/federal/us/425/435/.
[102] *Ibid*.
[103] *Id*. 442.
[104] *United States v. Miller*.

> A fortiori, he does not have standing to contest the Government's subpoena to the bank. … I wash my hands of today's extended redundancy by the Court.[105]

In a separate dissent, Justice Brennan warned of the danger inherent in permitting such broad and judicially unchecked surveillance. Especially prescient was his concern over the characterization of persons' provision of information to banks as "voluntary." He wrote:

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. … Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[106]

In the context of this proposed rulemaking, however, the expansion of recordkeeping requirements to persons who are neither customer agents nor principals would need to be judged right alongside the required reports. The two aspects of the rule taken together unquestionably require the seizure by brokers, so defined, of personal financial information that would never be shared but for the rule and is, therefore, *entirely* non-volitional.

There is not a single software developer today, of which we are aware, who is creating "unhosted wallet" software, but who also collects or seeks to to collect any of the personal identifying information contemplated to be reported in this rulemaking from the many strangers who choose to use that wallet software. That includes developers of "unhosted wallets" with software encoded "links or other mechanisms for direct access to third party services that allow users to buy and sell digital assets held in their unhosted wallets," software developers who would, under the proposed rule, be required to collect and report such information.[107]

Though the Court allowed the warrantless reporting in *Miller*, its holding was very clear. In that case the mandate to collect and report was not a seizure of *customer* records because it only

---

[105] *Id*. 455-456.
[106] *Id*. 451-452.
[107] *Supra* note 2.

"pertain[ed] to transactions to which the bank was itself a party."[108] It involved only information "voluntarily" handed over to the bank from its customers and that information was limited to conducting the "legitimate business purpose" of operating a bank (*e.g.* signatures on negotiable instruments, payment instructions, and the like). The Court's holding was also limited to the disclosure of information that was narrowly limited in numerosity, sweep, and nature.

A developer of an unhosted wallet or smart contract does not have any legitimate business purpose to collect information about the users of their software. Indeed, such collection is anathema to the business purpose in which the developer has presumably engaged: the publication of software with strong privacy and security guarantees (*e.g.* no back doors or surveillance). Nor would users be voluntarily providing this information to the developer if they were operating under the misapprehension that the software was delivering upon its stated purpose of enabling private transactions or cryptocurrency exchange without an intermediary. In effect, the users' information would be surreptitiously captured while they operated under the false belief that the tools they were using honored their expectations of privacy.

If a developer of such software publicly announced that they were voluntarily incorporating broker rule compliant surveillance into their tools, users who continued to use those tools would likely lose their reasonable expectation of privacy over any information they provided when they used those tools. However, it is hard to imagine that every developer of unhosted wallet or smart contract software would suddenly choose to voluntarily surveil the users of their software, even under pressure from U.S. law enforcement (many are not located in the U.S.). It is even more unbelievable that users would continue to use tools that had known backdoors if previous versions of the software without backdoors continued to exist in online archives, peer-to-peer file sharing networks, or the immutable blockchains themselves, or if other developers continued to offer more private alternatives.

Finally, it is important to remember that the constitutionality of the Bank Secrecy Act as adjudged in *Shultz* and *Miller* was only "as applied" in the implementing regulations of the 1970s.[109] Since the 1970s the BSA's reach has expanded both in the number of businesses it treats as financial institutions and in the quantity and type of transaction reports those financial institutions are required to file. To our knowledge, for example, the constitutionality of domestic SARs has never been challenged or vindicated. Neither has the application of the BSA to businesses that are not traditionally understood to be financial institutions, such as casinos or retail sellers of prepaid cards.

The tenuous nature of the BSA's constitutionality is underscored by the vote count in *California Bankers*. The majority opinion of the Court is matched with a concurrence authored by Justice

[108] *United States v. Miller*, 425 U.S. 435 (1976).
[109] *California Bankers Assn. v. Shultz*, 78-79.

Powell and joined by Justice Blackmun. Had these two justices sided with the dissenters the outcome would have been 5-4 against the BSA's constitutionality. Powell's concurrence specifically says that his opinion is predicated on the narrow application of the BSA that existed at the time:

> A significant extension of the regulations' reporting requirements, however, would pose substantial and difficult constitutional questions for me. In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate.[110]

Powell subsequently authored the majority opinion in *Miller*, but made clear that constitutionality was predicated on the narrowness of the investigation into Miller's moonshine operation and the judicial process that accompanied it:

> We are not confronted with a situation in which the Government, through "unreviewed executive discretion," has made a wide-ranging inquiry that unnecessarily "touch[es] upon intimate areas of an individual's personal affairs." *California Bankers Assn. v. Shultz*, 416 U.S. at 416 U. S. 78-79 (POWELL, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas duces tecum subject to the legal restraints attendant to such process.[111]

The present proposed rule would confront the Court with a situation in which the government makes a wide-ranging inquiry that unnecessarily touches upon intimate areas of every cryptocurrency user's personal affairs. *Miller* dealt with a single warrantless request made via a subpoena *duce tecum* subject to the legal restraints attendant to such process for bank records of a single suspect in an ongoing criminal investigation. In contrast, the Treasury Department's proposed rule would mandate the bulk collection and reporting of every transaction by every person using software to trade digital assets automatically and with no particular legal restraints on that process.

[110] *Ibid.*
[111] *United States v. Miller*, footnote 6.

Privacy interest of the users post-*Carpenter*

The Court has already encountered the above hypothesized limits to *Miller*. In *Carpenter v. U.S.*, the Court was faced with a warrantless request for customer information (cell site location information, CSLI) to a third party (the cellular network provider Sprint) by law enforcement agents investigating a crime. Faced with the fact that allowing the warrantless search would effectively rubber stamp the indiscriminate and warrantless collection of location history for any person with a cell phone, the Court enforced important limits on the third party doctrine.[112]

Rather than overrule *Miller*, the Court in *Carpenter* emphasized the voluntary nature of the information collection in *Miller*, distinguishing that collection from the arguably involuntary creation of CSLI as a byproduct of cell phone usage. The Court reasoned that the information was never voluntarily "shared" by customers because of the ubiquity of cell phones, their necessity to everyday life, and the fact that they simply cannot be used without revealing that data.[113] The Court found that, "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements."[114]

On the question of legitimate business purposes, the Court noted that in both *Miller* and *Smith v. Maryland* (a companion case dealing with warrantless searches of telephone records) the records in question were at the core of the legitimate business purpose of the third party.[115] A phone company *must know* the number that their customer wishes to reach. A bank *must know* the name of the person the customer wishes to pay. The warrantless data collection in those cases was limited to those key items that customers must understand as *essential* to their use of the business' services; items that a reasonable customer would expect the third party to have and retain. With cellular location data, however, the Court found that "there are no comparable limitations on the revealing nature" of the information sought.[116] A cell phone company need not know the customer's location at all times to connect calls, and subscribers would not expect them to have and retain this information as a condition of receiving cell service.

Customers understand that the numbers they ask to be connected with must be shared in order to be connected in a call. They do not contemplate trading the full revelation of their day-to-day movements merely because they wish to check their email. Interestingly, this holding does not argue that there is *no* legitimate business purpose that could justify the

[112] *Carpenter v. United States*, 585 U.S. ___ (2018).
[113] *Ibid*.
[114] *Ibid*.
[115] *Ibid*.
[116] *Ibid*.

telecommunications providers collecting and retaining that data (surely knowing where your customers are is important to providing them with good mobile phone connectivity).[117] Instead, it argues that the data sought by law enforcement was ancillary to the data that a customer would reasonably expect to provide within the context of the particular business relationship.[118] It is data that may be legitimate for the business to obtain, but it is not essential to the provision of the service and is beyond the business purpose as the customer understands it and therefore within her reasonable expectation of privacy.[119]

The technology behind an "unhosted wallet" or a decentralized exchange smart contract is designed to obviate the need for users to hand any personal data over to any third party. Indeed, these systems are designed such that no trusted third party need even exist for the transaction or exchange to take place. That is, after all, the point of cryptocurrency and "decentralized finance." Therefore, it would be impossible to argue that the users of these systems voluntarily hand any personal data over to any third party when they transact. A user will construct her electronic messages to be compatible with the software and smart contracts that she chooses to use, but this data alone will not be sufficient to fulfill the reporting requirements of this rulemaking because it never includes typical financial transaction data like the name or physical address of the user. Regardless of its lack of personal information, this is the only data that a user of these tools *must* provide in order to obtain the desired result and, consequently, it is the only data for which the user would no longer have a reasonable expectation of privacy.

No third party within these systems *must know* any additional information about the user for the transaction to take place; thus, it would be impossible to argue that such extra data was essential to the conduct of any supposed third party's business purposes.[120] Arguing the opposite is equivalent to suggesting that envelope manufacturers have a legitimate business purpose in learning what letters people mail, or that safe manufacturers have a legitimate business purpose in learning what valuables people keep in their safes.

Since *Carpenter* a handful of lower-court cases have dealt with the constitutionality of data collection in the context of cryptocurrency. None, however, are relevant to this discussion

[117] *Ibid*.
[118] *Ibid*.
[119] *Ibid*.
[120] *Ibid.*

because all of them deal with trusted and regulated cryptocurrency exchanges.[121] As we have argued, these entities *do* have a traditional brokerage-like relationship with their customers as a customer agent or principal and, accordingly, we do not object to their inclusion within the scope of the reporting obligations. No case has yet raised the question of whether a user of a trust-minimized tool like a software "unhosted wallet" or a decentralized exchange "smart contract" maintains a reasonable expectation of privacy over their personal information when using these tools for the simple reason that no developer of any such tools has ever collected such information and nor has a regulation yet demanded it. This rulemaking may be the first to provide the opportunity to create that case law.

This rulemaking and an alternative trespass theory of the Fourth Amendment

Carpenter was decided in 2018. There is a growing consensus, including among members of the Court, that the holdings in *California Bankers, Miller,* and *Smith,* which created the third party doctrine, should be rethought in light of modern technologies.

Justice Gorsuch was inclined to agree with the substantive outcome in *Carpenter*, but nonetheless offered a dissenting opinion that criticized "the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only Katz-squared." (referring to *Katz v. United States*, the case that originated the "reasonable expectation of privacy" test for whether a search has occurred). Gorsuch, following a scholarly path adopted by the Court in *United States v. Jones*,[122] instead favors an originalist interpretation of the Fourth Amendment that looks to traditional common law privacy principles, such as trespass, in order to parse and interpret the Fourth Amendment's privacy guarantees. This approach abandons the modern "reasonable expectation" standard from *Katz* in favor of an objective inquiry into whether the nature of the government intrusion is sufficiently analogous to an actionable trespass (as understood at the time of the founding) to warrant its characterization as a search.

In the context of intrusions upon private communications and transactions, an older line of cases already supplies the beginnings of a trespass-theory Fourth Amendment analysis. The

[121] See *Zietzke v. United States*. See also, *United States v. Gratkowski*. (The court in Gratkowski noted specifically that by using an agent to hold and trade bitcoin, customers knowingly gave up their privacy and suggested that a bitcoin user who refused to engage such an agent and who used software tools instead would retain a reasonable expectation of privacy. "Bitcoin users have the option to maintain a high level of privacy by transacting without a third-party intermediary. But that requires technical expertise, so Bitcoin users may elect to sacrifice some privacy by transacting through an intermediary such as Coinbase."). See also, *Harper v. Rettig*, Civil 1:20-cv-00771-JL, at *13 (D.N.H. May 26, 2023) (finding that users like the Plaintiff "sacrifice some privacy" and thus lack a protectable "privacy interest in the records of [their] [b]itcoin transactions on Coinbase" or other virtual currency exchanges.)..

[122] 565 U.S. 400 (2012).

primary case on point is *Ex Parte Jackson.*[123] *Ex Parte Jackson* dealt with the privacy of persons' papers while traveling through the mail. As the Court found,

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.[124]

The Court did not find that this "closure" against inspection needed to be impenetrable to be worthy of triggering a warrant requirement for search. As the Court held,

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.[125]

A digital asset exchange transaction sent from "unhosted wallet" software is the modern equivalent of a sealed envelope. The salient details of that transaction message, including who is paying who and how much, is absolutely "closed against inspection"[126] as that transaction is broadcast across a network.

Any evidence of an association between a transaction message and a real identity exists only within a computer located in the sender's home or else on her person. Any demand that such evidence be made available to law enforcement is indistinguishable from an actual intrusion into the home and a seizure of private records stored therein. As the Court found in *Kyllo v. United States*, in an opinion authored by Justice Scalia, it does not matter that the intrusion into the home is now occurring indirectly by use of sophisticated technology or that it is limited to a modicum of private information, or that the information is particularly intimate or mundane—all that matters is that the information sought was secured inside the home:

> [A sophisticated thermal imaging camera] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider "intimate"; and a much more sophisticated system might detect nothing

[123] *Ex parte Jackson*, 96 U.S. 727 (1878), https://supreme.justia.com/cases/federal/us/96/727/. Justice Gorsuch, in his *Carpenter* dissent, expresses no qualms with applying this "ancient" framework to modern technologies. *Carpenter v. United States* (Gorsuch, N., dissenting). ("These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents.").
[124] *Ex parte Jackson* 733.
[125] *Ibid*.
[126] *Ibid.*

> more intimate than the fact that someone left a closet light on. We could not, in other words, develop a rule approving only that through-the-wall surveillance which identifies objects no smaller than 36 by 36 inches, but would have to develop a jurisprudence specifying which home activities are "intimate" and which are not. And even when (if ever) that jurisprudence were fully developed, no police officer would be able to know in advance whether his through-the-wall surveillance picks up "intimate" details–and thus would be unable to know in advance whether it is constitutional.[127]

Irrespective of whether the Court in future cases maintains a *Katz* reasonable expectation of privacy theory of the Fourth Amendment or shifts to a property and trespass theory of the Fourth Amendment, this rulemaking, by deputizing mere software developers as state agents obligated to search and seize the private information of those who use their software, goes significantly beyond the bounds of the Constitution.

Conclusion

The extension of reporting obligations to persons who are not customer agents or principals in sales of digital assets to customers runs counter to the statutory authority found in the Infrastructure Investment and Jobs Act, the legislative history of that Act's passage, and—most importantly—would violate the First Amendment rights of cryptocurrency software, data, and website publishers, as well as the Fourth Amendment rights of both the publishers and the users of said software, data, and websites.

We therefore ask that the Treasury Department reconsider its proposed rule, and instead merely clarify that brokers, as traditionally defined, include those who effect sales of digital assets.

[127] *Kyllo v. United States*, 533 U.S. 27 (2001), https://supreme.justia.com/cases/federal/us/533/27/.