THEODORE H. FRANK (SBN 196332)

COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street, NW, 7th Floor
Washington, D.C. 20006
Tel.: 202.331.2263
Fax.: 202.331.0640

Attorney for *Amicus Curiae*
COMPETITIVE ENTERPRISE INSTITUTE

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Petitioner,

v.

COINBASE, INC.,

Respondent.

Case No. 3:17-cv-01431-JSC

BRIEF OF AMICUS CURIAE COMPETITIVE ENTERPRISE INSTITUE IN OPPOSITION TO PETITION TO ENFORCE INTERNAL REVENUE SERVICE SUMMONS

Courtroom: F (15th Floor)
Judge: Hon. Jacqueline Scott Corley

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The contract between Coinbase and its customers allocates property rights in personal information. That protects customers' privacy along many dimensions. The risks to Coinbase customers from the sharing of data with the government are substantial, requiring that any subpoena be tightly circumscribed.

The IRS issued a grossly overbroad subpoena and declined to narrow it until less than a month ago. This Court has wide latitude to limit or quash the subpoena even apart from the issues of improper purpose and abuse of process raised by Coinbase and intervenor John Doe 4.

The IRS's subpoena should be quashed in its entirety, not just narrowed. To do otherwise would reward the practice of issuing overbroad subpoenas as a sort of bargaining position that produces better results for the government than coming to court with a well-framed subpoena in the first instance. Given the high stakes for Coinbase users and the ease with which they can be notified, Due Process requires that they be directly notified if the subpoena survives in any form.

STATEMENT OF INTEREST OF *AMICUS CURIAE*

Founded in 1984, Competitive Enterprise Institute (CEI) is a public interest organization dedicated to protecting limited government and individual liberty. CEI, which is independent of the parties to this action (and has no ties to them), studies subjects relevant to this case, such virtual currencies, and the privacy and property implications of broad government data demands in the information age.

ARGUMENT

I. In Evaluating the IRS Subpoena, This Court Should Take Note of the Contract-Based Privacy Interests of Coinbase Users

A. The Coinbase Contract Allocates Information-Control Rights to Its Users

When people use digital financial and monetary services, they share and produce personal information that can be sensitive, intimate, and privileged. This is why the Coinbase user agreement and privacy policy, consistent with practice across digital services, allocate to customers the bulk of rights to control and use their personal data. These property rights in data include the right of users to exclude others from personal data in all but closely defined circumstances.

Both today and in 2015, Coinbase's User Agreement characterizes itself as a contract. "This is a contract between you and Coinbase, Inc." www.coinbase.com/legal/user_agreement. "This User Agreement ('Agreement') is a contract between you ('you,' 'your' or 'user') and Coinbase, Inc." https://web.archive.org/web/20150905173612/https://www.coinbase.com/legal/user_agreement [hereafter "2015 contract"]. The contract incorporates by reference the Coinbase privacy policy. 2015 contract, §7.3 ("Please review our Privacy Policy, which is hereby incorporated by reference into this Agreement…")

Coinbase's privacy policy is typical in that it denies Coinbase rights to use or sell the data except as provided in the policy. "Coinbase will not sell or rent any of your personal information to third parties for their marketing purposes and only shares your personal information with third parties as described in this policy." 2015 contract. This leaves the right to exclude all others from the data with the customer. The possessive pronoun "your" signifies that the bulk of the ownership of the data is the customer's.

These rights are property rights within the meaning of the Constitution's guarantees of individual rights. *See United States Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977) ("Contract rights are a form of property"). There is no juridical way to characterize Coinbase's arrangements with customers other than as contracts allocating property rights.

The exceptions to user ownership, allocating certain rights to Coinbase, are also typical of privacy policies. Coinbase may share personal information with service providers, financial institution partners and merger partners—all subject to relevant constraints. Coinbase may share information with other third parties "with your consent or direction to do so," 2015 contract, reiterating that the right to sell, like the bulk of the rights to the data, rests with the customer.

One of the exceptions—also typical (and appropriate)—is the exception for sharing with government and law enforcement. That provision states in relevant part: "We may share your personal information with … [l]aw enforcement, government officials, or other third parties when … [w]e are compelled to do so by a subpoena, court order, or similar legal procedure."

2015 contract.

This provision does not give Coinbase free rein to hand data over to the government when asked. Coinbase can only do so when "compelled."

That strong term, "compelled," implies that the process must overcome resistance. Coinbase is obligated by the contract to resist invalid subpoenas, as in the instant case. Coinbase would be justified in declining to put up faux resistance to clearly valid procedures, of course.

But Coinbase is rightly resisting in this case. And to the extent Coinbase does not resist an invalid or overbroad subpoena, the data is not Coinbase's to turn over. It remains the property of the customer. That is why, though currently acting in parallel, the intervenors in this case have interests distinct from Coinbase's.

The contract also provides that any procedure must be "legal." At least two senses of that word are relevant. One is that the procedures are recognized and systematically used procedures in law enforcement and courts. The other is that the procedures comport with the standards laid out in the law. The contract does not permit Coinbase to comply with subpoenas simply because they take a certain form. They must also satisfy the substantive legal merits for divesting a private party of control over the things the government demands. Coinbase has the right to share the data only if the process used to divest the customer of control is legal in both form and substance.

The reason for all this is the protection of privacy and related interests.

B. Coinbase Customers Safeguard Their Privacy Interests by Controlling Their Information

Control of information through contract is a means to many important ends, clustered around the concept of "privacy." These significant Coinbase customer interests would be upset by the granting of the subpoena, even in pared-down form. These interests justify limits on even subpoenas seeking relevant information. *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 683 (N.D. Cal. 2006).

There are many dimensions of "privacy."[1] This amicus will emphasize four here: control, security, freedom of speech and action, and privilege.

1) Arguably at the heart of information privacy is the base notion of autonomy—of having control over one's life. Coinbase users enter into dealings with Coinbase expecting information controls to come with the digital services provided. Such controls help make people autonomous agents in a rule-bound environment as opposed to pawns of corporations and governments.

2) Particularly in the area of financial services, privacy is a means to important security ends. If the knowledge of a person's wealth or assets is available broadly, this raises the risk that criminal individuals or enterprises may target them for burglary, fraud, or even kidnapping. For many people, asset amounts, locations, and characterizations are extremely important to keep confidential. Digital data is subject to hacking and breach, no matter who has custody of it, so risks of fraud, theft, and literal physical harm rise with each data holder and copy of data.

As the intervenors note, the IRS has been criticized by the Treasury Department's own inspector general "for its inability to protect victims of a prior hack of IRS computers" and "ignoring the palpable risks that it could be hacked again, which could cause Coinbase customers to lose their virtual currency forever." *See* ECF No. 10, Mot. at 21.

All this counsels for stringently minimizing the extent of forced information-sharing. The risks associated with data have grown since the days of paper, when Congress passed the John Doe statute.

3) Financial information is a window onto the activities and priorities of individuals. And seizure of financial information can act as a brake on freedom of speech and action. Bitcoin transaction records include wallet addresses that can later be linked to real-world senders and recipients. This makes them potentially as revealing as any log of a person's activities, interests, and attitudes. The Coinbase users whose data are subject to the subpoena may have made donations to charitable or controversial causes, for example. They may have paid for stigmatized

[1] A useful summary of many issues can be found at https://plato.stanford.edu/entries/privacy/.

medical or mental health services, or used Bitcoin to pay for goods or services that relate to sexual, marital, or family relations. Seizure of data en masse from a large number of Coinbase users will likely have chilling effects on the speech and action of both current and future users.

Chilling effects matter, because when a subpoena chills a person's constitutionally protected speech, *see, e.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (anonymous speech), the requester must show a compelling interest in obtaining the information it seeks and must articulate a substantial nexus between the information sought and the compelling interest. *Gibson v. Florida Legis. Investigation Comm.*, 372 U.S. 539, 546 (1963); *cf. Gonzales v. Google, Inc.*, 234 F.R.D. 674, 687 (N.D. Cal. 2006) (considering *sua sponte* the privacy interests of Google users to limit request to Google seeking information about users' Internet searches). Even the risk of disclosure of reading or viewing preferences triggers First Amendment scrutiny. *See Denver Area Educ. Telecomms. Consortium, Inc. v. FCC*, 518 U.S. 727, 754 (1996) (requirement that people wishing to receive patently offensive programming provide "written notice" to the cable operator violated the First Amendment, because it "will further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the patently offensive channel"); *Lubin v. Agora, Inc.*, 882 A.2d 833, 845 (Md. 2005) (investment newsletter subscriber lists protected by First Amendment against subpoena in securities-fraud investigation).

Given the kinship among speech surveillance, financial tracking, and location tracking—all potentially chill speech and constitutionally protected action—the words of U.S. Supreme Court Justice Sonia Sotomayor in *United States v. Jones*, a GPS tracking case, illustrate how to think about data privacy and freedom:

"Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *United States* *v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

4) Finally, privacy of financial information is a significant dimension of certain relationships that are privileged by law. Payments to attorneys can reveal the existence, nature, and type of legal services a person is engaging. Data about people's Bitcoin transactions may not reveal such things immediately, but given the permanency of blockchain records, future acquisitions of data by the IRS or other governmental entities may reveal connections that produce inferences about legally privileged relationships that the government is not entitled to know about.

Coinbase has parallel interests to its users'. The requesting party must show a substantial need for the material sought by a subpoena if it would have "an appreciable impact" on customers' use of the company due to erosion of their privacy. *Gonzales v. Google, Inc*., 234 F.R.D. 674, 684 (N.D. Cal. 2006). Such interests do not need rise to the level of enforceable contractual or constitutional rights to justify modifying or quashing a subpoena, and are relevant even if a business has "not suggested to its users" that their information will be "kept confidential," and their "expectation of privacy" is thus "not entirely reasonable." *Id.* If "the frequency with which users" use a business's services would be harmed by forcing production of the information sought by the subpoena, "[t]he burden thus shifts to the Government to demonstrate that the requested discovery is relevant and essential." *Id.* at 685.

Here, the subpoena is even more problematic than in the *Google* case. Coinbase's terms of service and privacy policy have not just "suggested," but expressly promised that it would keep confidential the information now demanded by the government.

Disclosure also will cause much more harm to Coinbase than the subpoena in the *Google* case could have caused that company. Google continues to be the most widely used Web search engine despite occasional instances of compelled production of even highly personal user data. Coinbase's businesses may be gravely harmed by compliance with the subpoena. The "loss of goodwill" if Coinbase is forced to disclose this information, *see Google,* 234 F.R.D. at 684, is likely far greater than was the case for Google. It was improper for the IRS to disregard these privacy, property, and data-intensive business interests in drafting its sweepingly broad subpoena.

Privacy interests would not defeat a well-crafted subpoena tailored to discover the identities of persons about whom there is a genuine suspicion of failure to pay taxes. But the subpoena at issue here does not meet that standard, and this Court should reject it.

II. The Subpoena Should Be Quashed Outright Due to Its Original Vast Overbreadth

This Court should quash the IRS's subpoena outright. It can do so in circumstances such as this in order to discourage litigants from wasting judicial resources by issuing overbroad subpoenas, then tailoring them based on the reaction of courts and litigants. The government's overbreadth in the original subpoena should not be rewarded through the enforcement of a less overbroad—but still broad—subpoena. The tardily pared-back subpoena remains overbroad, as it still lacks the focus required by the statute. This Court can quash or limit a subpoena even without a showing of improper motive.

A. This Court Can Quash the Subpoena in Its Entirety

Where the issuer of a subpoena issues a grossly overbroad subpoena and declines to narrow it until long after sound objections have been raised, the court can and should quash the entire subpoena, even if it could theoretically be narrowed. Doing otherwise "would 'encourage litigants to demand the moon thinking they can always fall back to something reasonable. They should be reasonable from the start.'" *Boston Scientific Corp. v. Lee*, 5:14–cv–mc–80188–BLF–PSG, 2014 WL 3851157, at *7 n.59 (N.D. Cal. Aug. 4, 2014), *quoting Straight Path IP Group, Inc. v. Blackberry Limited*, 2014 WL 3401723, at *5 (N.D. Cal. July 8, 2014).

The *Boston Scientific* decision cited an earlier ruling of this Court, which similarly refused to enforce an overbroad subpoena at all, rather than narrowing it. As that earlier ruling noted, had the issuer of the subpoena "served only a request to authenticate a few dozen specifically identified documents, the subpoena would likely have been enforced. But the subpoena served was exponentially more burdensome. The swath of the subpoena is so burdensome that it would be bad policy to now whittle it back to something narrow and reasonable. Instead, the baby should go out with the bath water—the entire defective subpoena will be quashed in its entirety." *Straight Path IP Group, Inc. v. Blackberry Limited*, Case No. 3:14–mc–80150–WHA, 2014 WL 3401723, at *5 (N.D. Cal. July 8, 2014).

Where a subpoena is grossly overbroad, a court has the discretion to quash it in its entirety. *See, e.g.*, *Katz v. Batavia Marine & Sporting Supplies*, 984 F.2d 422, 425 (Fed. Cir. 1993) (where "description of the documents to be produced, on their face, exceed the" scope of the issue being litigated, "the district court did not abuse its discretion in denying the requested discovery, on the ground that [the requester] had not shown a need for the broad range of information requested"); *EEOC v. Burlington Northern Santa Fe Railroad*, 669 F.3d 1154, 1157 (10th Cir. 2012) (upholding trial court's refusal to enforce a subpoena seeking pattern-or-practice information after individual complaint of discrimination, because the issue being litigated did not justify such "an incredibly broad request for information"); *General Insurance Co. v. EEOC*, 491 F.2d 133, 136 (9th Cir. 1974). This is true even if some kernels of the information sought are relevant, because *"[e]ven if relevant*, discovery is not permitted where no need is shown, or compliance would be unduly burdensome, or where harm to the person from whom discovery is sought outweighs the need of the person seeking discovery of the information." *Micro Motion, Inc. v. Kane Steel Co.*, 894 F.2d 1318, 1323 (Fed. Cir. 1990) (quashing subpoena in its entirety even though some of what it sought was theoretically relevant or relevant to alternative theories of recovery; citing FRCP 26(b)(1)).

The speculative "hope that something may be discovered" through a subpoena, *David H. Tedder & Assocs. v. United States*, 77 F.3d 1166, 1168–69 (9th Cir. 1996), is insufficient to validate it. The Fourth Amendment forbids a "fishing expedition" even when "some part of the presumably large mass of papers" sought may end up showing wrongdoing. *FTC v. American Tobacco*, 264 U.S. 298, 307 (1924).

B. The Original Subpoena Was Extremely Overbroad

As this Court has recognized, under the sweeping rationale offered for its original subpoena, "the IRS could subpoena every single bank record in the country." Woods Decl., Exh. 7 (Transcript of Proceedings), at 13:8-10. It could issue "a subpoena to Bank of America for every single account that it has." *Id.* at 7:8-12. Just about every institution has some customers who are potential tax evaders. The subpoena was vastly broader than the subpoenas the IRS customarily issues to financial institutions, and it demands types of information never the subject of IRS reporting requirements (such as communications between customers and Coinbase).

Here, the subpoena did not target any specific taxpayers, or even a definable class of taxpayers that the IRS believes have underpaid taxes, despite the requirement that a John Doe subpoena must target an "ascertainable group or class of persons" suspected of failing to "comply with" their tax obligations. 26 U.S.C. § 7609(f). Instead, the IRS's original subpoena demanded information "[f]or each Coinbase user," see Utzke Decl., Ex. A, p. 6, and it claimed to be investigating every single "United States person who conducted transactions in a convertible virtual currency" over a three-year period. Utzke Decl. That "covers millions of customer accounts." Brian Armstrong, *Coinbase and the IRS*, Medium.com, Jan. 14, 2017, https://medium.com/@barmstrong/coinbase-and-the-irs-c4e2e386e0cf.

Many of these Coinbase users obviously did not owe tax, much less evade any taxes. There is no tax on mere possession of Bitcoin, and transactions in Bitcoin are only relevant if they result in an overall taxable gain. *See* IRS Notice 2014-21 (Utzke Decl., Ex. B, at A-1, A-6).

The overbreadth of the subpoena was repeatedly noted by scholars and commentators. "Should the Internal Revenue Service (IRS) have authority to make financial-services companies turn over millions of customer records when they suspect a handful of customers could be evading taxes? Most people would respond with an emphatic *no*, yet this is exactly what the IRS is attempting to do with Coinbase," threatening "online privacy" and the "digital privacy of all Americans," noted Andrea O'Sullivan, a program manager with the Technology Policy Program at George Mason University's Mercatus Center, in January.[2] "Americans would be shocked if the IRS asked a financial institution in good regulatory standing to turn over the names, addresses and shopping histories of millions of customers just because the IRS thought there might be some tax cheats among them. But that's exactly what the IRS did," a prominent

[2] Andrea O'Sullivan, *How the IRS Could Cripple Cryptocurrency*, Reason, January 24, 2017, http://reason.com/archives/2017/01/24/the-irss-war-on-coinbase.

member of the digital currency community, Jerry Brito, noted in *The American Banker*.[3]

The IRS later confessed to overbreadth, first by agreeing not to seek password and security settings for Coinbase users' accounts, and then by belatedly filing a Notice of Narrowed Subpoena on July 6. ECF No. 37. But it continues to seek a great deal of irrelevant information about Coinbase users who have not plausibly failed to report any taxable income on Bitcoin.

And it was unusually tardy in narrowing the subpoena. That happened after it became obvious at the Court's June 29, 2017 hearing that the Court would not enforce the subpoena in its original form, or anything close to it. Coinbase users had much earlier pointed out that "the categories of requested documents were so overbroad such that the IRS Summons would require the disclosure of a substantial amount of wholly irrelevant information and documents." Intervenor John Doe 4's Opposition to Petition (ECF No. 44) at 5. In May 2017, three senior members of Congress warned the IRS that its subpoena was "overly broad, extremely burdensome, and highly intrusive" and potentially "dangerous." Coinbase Inc.'s Opposition to Petition (ECF No. 46) at 6; Woods Decl., Exh. 5.

Despite these significant rebukes, the IRS persisted with its unprecedentedly broad subpoena until this Court questioned the extraordinarily "broad swath" of information it demanded at the June 29 hearing, Coinbase Opp. At 7, which was so sweeping that under its logic "the IRS could subpoena every single bank record in the country." Woods Decl., Exh. 7 (Transcript of Proceedings), at 13:8-10.

Even if the subpoena had not demanded the information of such a vast number of people—over a million customers—it would still be overbroad. Demanding data on all customers when merely a subset would suffice is a classic example of overbreadth. *E.g.*, *Ex parte Mobile Fixture & Equipment Co.*, 630 So.2d 358, 360 (Ala. 1993) (denying request for production of information on defendant's investigations of employees and customers, which would require it to reveal names, addresses, and phone numbers of its customers, and review

[3] Jerry Brito, *IRS Quest for Coinbase Data Sets Dangerous Precedent*, American Banker, Nov. 29, 2016, www.americanbanker.com/opinion/irs-quest-for-coinbase-data-sets-dangerous-precedent.

5,400 files); *Ex parte Compass Bank*, 686 So.2d 1135, 1138 (Ala. 1996) (judge abused his discretion in ordering production of every one of 21,246 customer files, which "would be unduly broad, burdensome"); *SIPC v. Bernard L. Madoff Inv. Securities*, 496 B.R. 713, 726 (S.D.N.Y. 2013) (seeking records on "all allowed customers" was overbroad); *Boucher v. First American Title Ins. Co.*, No. C10–199RAJ, 2011 WL 5299497, *5 (W.D. Wash. Nov. 4, 2011) (demanding "name and address of every customer over the last eight years" was excessive); *Ex parte Henry*, 770 So.2d 76, 80 (Ala. 2000) (request for "name of every person who had purchased a life insurance policy" was "overly broad" in fraud case); *In re Broiler Chicken Antitrust Litig.*, No. 1:16-cv-08637, 2017 WL 1682572, *1 n.2 & *6 (N.D. Ill. April 21, 2017) (demand for information on "very large number of Defendant's customers" was too broad).

Data demands, such as the subpoenas in this case, are not permitted to impose the same degree of burden that is permissible in discovery between parties to pre-existing litigation, as was the case in the rulings cited above. *See Dart Indus. Co. v. Westwood Chem. Co.*, 649 F.2d 646, 649 (9th Cir. 1980) (subpoenas should "be more limited" than document demands between parties to pre-existing civil litigation in order "to protect" recipients "from harassment, inconvenience, or disclosure of confidential documents").

The IRS demanded "[a]ll correspondence between Coinbase and the user," regardless of their form, subject matter, and whether they have any conceivable relationship to one's tax liability. See Utzke Decl., Ex. A., ECF No. 1-2 at 6 (request No. 6).

C. The Subpoena Remains Overbroad

Even now, the IRS continues to seek information on Coinbase users who don't owe any tax on their bitcoin. For example, under its narrowed subpoena, "[t]he IRS has asked for the records of an account holder who, in a single year, bought $20,000 in Bitcoin and sold $5 worth of Bitcoin." *Opposition to Petition to Enforce Summons* at 21. During much of the period the subpoena covers, Bitcoin prices fell, resulting in losses on Bitcoin sales.

The purposes for which Congress authorized a subpoena are: "ascertaining the correctness of any return, making a return where none has been made, determining the liability of any person [or fiduciary] for any internal revenue tax …, or collecting any such liability." 26

U.S.C. § 7602(a). The statute does not invite or permit bulk data collection from a broad class of people, whether millions or thousands, based on the theory that some among them may have incorrect returns or outstanding liabilities. Instead, the government must show a tight relationship between the terms of its information demand and particular individuals, known by name or not.

D. This Court Can Quash an Overbroad Subpoena Even Without a Showing of Improper Motive

Although the IRS's subpoena power under 26 U.S.C. § 7609(f) is expansive, it does not justify enforcement of an overly broad or unduly burdensome subpoena. *United States v. Sepenuk*, 864 F.Supp. 1002, 1007 (D. Or. 1994) (refusing to enforce request in IRS subpoena that was "overly broad in scope"). Its subpoena can be challenged on "any appropriate ground," not just improper purpose or abuse of process. *See United States v. Sidley Austin Brown & Wood LLP* ("*Sidley Austin*"), No. 03 C 9355, 2004 WL 816448, at *9 (N.D. Ill. Apr. 15, 2004) ("The party can challenge the summons on any appropriate ground. Defenses to enforcement include disproving the existence of one of the *Powell* factors, showing the IRS issued the summons in bad faith, or asserting that the summons is ambiguous, vague, or otherwise deficient…").

Indeed, a court "must" quash or modify a subpoena that "subjects a person to undue burden." Fed. R. Civ. P. 45(d)(3)(iv). That includes an overbroad subpoena. A court will find a subpoena imposes an undue burden if it makes overbroad requests. *Wiwa v. Royal Dutch Petroleum Co.*, 392 F.3d 812, 818 (5th Cir. 2004); *see Tiberi v. CIGNA Ins. Co.*, 40 F.3d 110, 112 (5th Cir. 1994) (quashing overbroad subpoena rather than using "lesser remedy" of modification). The fact that *some* of the information it seeks may be relevant does not prevent it from being overbroad. Discovery requests are overbroad when only a fraction of the many documents requested are relevant, even if some responsive information is conceivably relevant. *Nugget Hydroelectric L.P. v. Pacific Gas & Elec. Co.*, 981 F.2d 429, 438–39 (9th Cir. 1992). "A subpoena duces tecum may not lawfully require the production of a mass of books and papers, merely so that one may search through them to gather evidence; and an omnibus subpoena for all, or even a substantial part, of the books and records of the subpoenaed party is invalid." *Imparato v. Spicola*, 238 So.2d 503, 511 (Fla. Dist. Ct. App. 1970).

"*Even if relevant*, discovery is not permitted where no need is shown, or compliance would be unduly burdensome, or where harm to the person from whom discovery is sought outweighs the need of the person seeking discovery of the information." *Micro Motion, Inc. v. Kane Steel Co*., 894 F.2d 1318, 1323 (Fed. Cir. 1990) (emphasis in original). The "court may modify or quash a subpoena even for relevant information if it finds that there is an undue burden on the non-party." *Gonzales v. Google, Inc.,* 234 F.R.D. 674, 683 (N.D. Cal. 2006). "Rule 45(c)(3)(B) provides additional protections where a subpoena seeks…confidential commercial information from a nonparty." In such cases, "the requesting party" must, among other things, "show a 'substantial need for the testimony or material that cannot be otherwise met without undue hardship." *Id.* at 684.

Nothing in the language of Rule 45 requires the recipient of a subpoena to show an improper purpose to obtain a court order quashing it. *See Mount Hope Church v. Bash Back!*, 705 F.3d 418, 428 (9th Cir. 2012) (bad faith is not required, but is sufficient for sanctions).

This Court has wide latitude to rule on the subpoena. The best option is to quash it in whole. Should the subpoena survive, Due Process requires notice to affected Coinbase users.

III. If This Court Views the Subpoena as Satisfying the 1976 John Doe Statute, It Should Consider Whether That Statute Violates Due Process Today

At the time Congress passed it, the "John Doe" provision of the Internal Revenue Code, 26 U.S.C. § 7609, may have been an appropriate measure for administering investigations of taxpayer delinquency. The "John Doe" statute does not satisfy the requirements of Due Process today. In 1976, it would have been highly burdensome to identify and contact individuals affected by a subpoena aimed at a group identified by class characteristics. Relating their membership in the class to their names and contact information would have been laborious and costly. Communicating with them would have required printing letters and envelopes, folding paper, sealing envelopes, and affixing postage stamps to pay for having them delivered through the postal mail. These costs would quickly mount up. In the digital era, that is no longer true.

The interests of "John Does" were lower in the technological context of 1976, too. The transfer of literal paper documents to one government bureau did not create risks like those that exist when digital data is shared today. When digital data is transferred to a new party, many additional copies of the same information are often created and distributed across technical systems. Whether intentionally or not, the data may come into many more hands than paper documents ever risked. In the era of paper, a single document given to a government bureau was unlikely to result in access by an untold number of fraudsters and criminals across the planet. Digital data carries greater risks to data subjects, making it more important than it was when the "John Doe" statute was passed to accord them the opportunity to contest the sharing of their data with others.

"Due process of law is [process which], following the forms of law, is appropriate to the case and just to the parties affected. It must be pursued in the ordinary mode prescribed by law; it must be adapted to the end to be attained; and whenever necessary to the protection of the parties, it must give them an opportunity to be heard respecting the justice of the judgment sought." *Hagar v. Reclamation Dist.*, 111 U.S. 701, 708 (1884). Should the subpoena survive in any form, it would be relatively easy and inexpensive to communicate by email with affected Coinbase customers. Doing so would be a practical measure, designed for protection of the parties by giving them the opportunity to be heard. The suggestion of Coinbase that its users should be accorded the right to participate is well taken. Indeed, it is demanded by principles of Due Process.

CONCLUSION

Coinbase and its users have allocated property rights in data among themselves by contract. Coinbase users have legitimate privacy interests they protect using their control of personal data, and Coinbase has a related business interest in protecting users. The IRS's hugely overbroad subpoena was a dagger aimed at the heart of the Coinbase/customer relationship and the interests and rights of both. Had the IRS come to the Court with a well-crafted subpoena premised on a genuine and valid theory that a discrete class of Coinbase users have been remiss with specific responsibilities or obligations, such subpoena would probably have passed muster. But the original subpoena did not, and the tardily pared-back subpoena does not.

This Court need not find an improper motive in order to limit or quash the subpoena. It can quash the subpoena in its entirety in the interest of proper judicial administration of the John Doe subpoena process. This Court should ensure that the government does not develop a strategy of serving distended subpoenas and using a judicially-refereed negotiating process to arrive at "better" results than what it could get with a well-tailored subpoena.

Given the acute interests of Coinbase users and the ease of notifying them so that they can participate in this matter, Due Process requires that all affected users should be given direct notice of this matter if the subpoena survives in any form.

Respectfully submitted,

Dated: August 3, 2017

By: /s/ Theodore H. Frank

THEODORE H. FRANK (SBN 196332)
Counsel of Record
Ted.Frank@cei.org
JIM HARPER
Jim.Harper@cei.org
HANS BADER
Hans.Bader@cei.org
SAM KAZMAN
Sam.Kazman@cei.org
COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street, NW, 7th Floor
Washington, D.C. 20006
(202) 331-2263

Attorneys for *Amicus Curiae*
COMPETITIVE ENTERPRISE INSTITUTE

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States District Court for the Northern District of California by using the CM/ECF system on **August 3, 2017**. I further certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

I certify under penalty of perjury that the foregoing is true and correct. Executed on **August 3, 2017**.

/s/ Theodore H. Frank____
THEODORE H. FRANK