NO. 25-1201

In the Supreme Court of the United States

NATIONAL SMALL BUSINESS UNITED, D/B/A NATIONAL SMALL BUSINESS ASSOCIATION, ET AL.,

Petitioners,

v.

SCOTT BESSENT, SECRETARY OF THE TREASURY, ET AL.,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

BRIEF OF AMICI CURIAE SMALL BUSINESS ASSOCIATION OF MICHIGAN AND CHALDEAN CHAMBER OF COMMERCE IN SUPPORT OF PETITIONERS

Stephen J. van Stempvoort
Counsel of Record
D. Andrew Portinga
Amanda L. Rauh-Bieri
MILLER JOHNSON
45 Ottawa Avenue SW, Suite 1100
Grand Rapids, MI 49503
(616) 831-1700
vanstempvoorts@millerjohnson.com

May 21, 2026 *Counsel for Amici Curiae*

SUPREME COURT PRESS ♦ (888) 958-5705 ♦ BOSTON, MASSACHUSETTS

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES (Cont.)

TABLE OF AUTHORITIES (Cont.)

CONSTITUTIONAL PROVISIONS

STATUTES

JUDICIAL RULES

REGULATIONS

TABLE OF AUTHORITIES (Cont.)

TABLE OF AUTHORITIES (Cont.)

INTEREST OF THE AMICI CURIAE[1]

The SMALL BUSINESS ASSOCIATION OF MICHIGAN ("SBAM") is a statewide organization for small business owners in Michigan, with over 32,000 members. SBAM's mission is the success of Michigan's small businesses, and it frequently advocates on public policy issues affecting small business owners.

The CHALDEAN AMERICAN CHAMBER OF COMMERCE (the "Chaldean Chamber") advocates and promotes small businesses and economic opportunities, particularly for businesses and individuals who are affiliated with the Chaldean-American community. Chaldeans are Aramaic-speaking, Eastern-Rite Catholics indigenous to Iraq. More than 4,000 businesses are members of the Chaldean Chamber.

Amici's interest in this case arises from their concerns regarding the Corporate Transparency Act's impact on small businesses. The CTA requires millions of law-abiding Americans, including SBAM's and the Chaldean Chamber's members, to report sensitive, private information to law enforcement without any suspicion of wrongdoing.

---

[1] No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae or its counsel made a monetary contribution to its preparation or submission. As required by Supreme Court Rule 37.2, counsel of record received timely notice of amici's intent to file this brief at least 10 days prior to its due date.

The CTA substantially impacts amici's members. FinCEN estimates that each reporting company's cost of filing the initial beneficiary ownership interest report will range from $85.14 to $2,614.87.[2] Based on those estimates, the total cost of compliance for SBAM's 32,000 members will be between roughly $2.5 million and $78.4 million, and the total cost of compliance for the Chaldean Chamber's 4,000 members will be between approximately $340,000 and $10.5 million. On a national scale, FinCEN estimates that the cost of compliance will be about $21.7 billion in 2024 and around $3.3 billion each year afterward.[3]

Because of these and other concerns, amici and other plaintiffs filed a constitutional challenge to the CTA in the U.S. District Court for the Western District of Michigan. The district court ruled in amici's favor, finding that the CTA violated the Fourth Amendment. *See Small Bus. Ass'n of Michigan v. Yellen*, 769 F. Supp. 3d 722 (W.D. Mich. 2025).

---

[2] *See* Beneficial Ownership Information Reporting Requirements for Financial Crimes Enforcement Network (FinCEN), 87 Fed. Reg. 59498, 59573 (Jan. 1, 2024), available at https://www.federalregister.gov/d/2022-21020/p-958.

[3] *See id.*

INTRODUCTION AND SUMMARY OF THE ARGUMENT

The Corporate Transparency Act ("CTA") compels millions of individuals and entities to divulge their private information to the Financial Crimes Enforcement Network ("FinCEN") so that law enforcement officers can rummage through it for evidence of criminal activity, without any suspicion that anyone in particular has committed a crime. Neither the government nor the lower courts dispute that the CTA's disclosure obligations are a Fourth Amendment search. The Eleventh Circuit nevertheless ruled that *California Bankers Association v. Shultz*, 416 U.S. 21 (1974), not only is a stand-alone exception to the warrant requirement but also applies to the CTA. The court held that the government can subject millions of law-abiding people to invasive searches of private information, even though the government's primary purpose is to obtain evidence in support of a criminal investigation.

Although the Eleventh Circuit's holding directly conflicts with *Small Business Association of Michigan v. Yellen* (*SBAM*), 769 F. Supp. 3d 722 (W.D. Mich. 2025), which invalidated the CTA on Fourth Amendment grounds, the Eleventh Circuit never addressed that case. And the implications of the Eleventh Circuit's ruling are significant. If the CTA's mandatory, suspicionless searches are acceptable under *Shultz*, then governments may compel the involuntary disclosure of private information from every citizen in the United States for criminal investigation purposes without suspicion

merely by characterizing the disclosure as a "reporting requirement." Upholding the CTA would fundamentally change the way in which the government collects information about American citizens and uses it against them. The petition should be granted.

ARGUMENT

I. The CTA Violates the Fourth Amendment.[4]

A. The CTA's Disclosure Requirements Are a Search for Purposes of the Fourth Amendment.

Although everyone agrees that the CTA's compelled disclosures are Fourth Amendment "searches," the Eleventh Circuit's analysis underappreciated the nature of the search at issue. The Fourth Amendment "is not confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process," including disclosures that are compelled by statute or regulation. *United States v. Morton Salt Co.*, 338 U.S. 632, 651-52 (1950); *see also City of Los Angeles v. Patel*, 576 U.S. 409, 412 (2015).

1. The CTA Effects a Search Under the Property-Based Test.

The "traditional" understanding of the Fourth Amendment is a property-based one. *Byrd v. United States*, 584 U.S. 395, 403 (2018). Under that property-

[4] Although amici agree with petitioners that the CTA is flawed on Commerce Clause grounds, the focus of this brief is on the Fourth Amendment. *See SBAM*, 769 F. Supp. 3d at 722.

based approach, the CTA effects a Fourth Amendment search because it mandates the disclosure of information that belongs to the reporting entities or their beneficial owners. *SBAM*, 769 F. Supp. 3d at 730-33. The CTA compels entities to disclose the identity of individuals who have "substantial control" over them —that is, to reveal the internal power dynamics of those entities. That corporate information belongs to those entities and individuals. *Hale v. Henkel*, 201 U.S. 43, 76 (1906) (corporate records are "papers" for purposes of the Fourth Amendment). And both individuals and corporate entities possess robust Fourth Amendment rights over their property and records. *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920); *accord G.M. Leasing Corp. v. United States*, 429 U.S. 338, 353 (1977). "To hold otherwise would belie the origin of that Amendment," which derived its core protections from the colonists' experience with British harassment of "merchants and businessmen . . . " *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 311-12 (1978).

It makes no difference that law enforcement agents do not physically arrive on reporting entities' premises and take photographs of corporate ledgers. *See Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 482-83 (S.D.N.Y. 2019) (collecting cases). The Fourth Amendment cannot be sidestepped by forcing entities and individuals to transcribe the most salient portions of their "papers" into a database, so long as the government leaves the physical documents in the entity's possession. *Brock v. Emerson Elec. Co., Elec. & Space Div.*, 834 F.2d 994, 996 (11th Cir. 1987); *see also Olmstead v. United States*, 277 U.S. 438, 474-75 (1928) (Brandeis, J., dissenting).

2. The CTA Intrudes on Entities' and Individuals' Reasonable Expectations of Privacy.

The CTA's required disclosures are a Fourth Amendment search under the "reasonable expectation of privacy" test, as well. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). A privacy interest "normally attaches to commercial information." *Brock*, 834 F.2d at 996. "[A]n individual in a business office," just like "a person in a telephone booth," is entitled to assume that his or her private conversations and decisions "will not be broadcast to the world." *Katz*, 389 U.S. at 352; *see also Free Speech Coalition, Inc. v. Att'y Gen. United States*, 825 F.3d 149, 168 (3d Cir. 2016).

Disclosing whether someone exercises "substantial control" over a corporate entity reveals information internal, and private, to that entity. A corporate entity's "arrangements," "understandings," "relationships," and other "direct" and "indirect" decision-making mechanisms for running the organization, 31 U.S.C. § 5336(a)(3)(A), are not aired publicly in the normal course of the entity's affairs. They happen *within* that corporate entity—privately—and their disclosure under the CTA requires the entity to reveal important and otherwise non-public information about its operations.

The CTA's definitions of "ownership" and "substantial control" require disclosures that extend far beyond existing ownership interests. The CTA, for example, requires disclosure of contingent future ownership interests, such as option agreements, warrants, or convertible notes. (FinCEN FAQ D.4, available at https://www.fincen.gov/boi-faqs#D_4). None of that infor-

mation is publicly available. And there are many reasons why an entity might wish to keep this information private. Public knowledge that a particular venture is (or is not) backed by either a famous or an infamous public figure, for example, might affect the company's ability to enter into certain contracts or arrangements. Or the entity might be concerned that a particular individual's involvement, if known, could invite political retaliation or increased (and perhaps unjustified) scrutiny from law enforcement.

The Eleventh Circuit's notion that American citizens have only modest expectations of privacy in their corporate records fails to appreciate that small business owners are not obligated to share this information with anyone outside the company. *Byrd* held that even an unauthorized driver of a rental car has a reasonable expectation of privacy in the vehicle by virtue of his ability to exclude carjackers from the vehicle. *Byrd*, 584 U.S. at 407. A corporate entity possesses the far more potent ability to exclude all individuals who are outside the company from being privy to its internal dynamics.

3. The Third-Party Doctrine Does Not Apply.

The third-party doctrine plays no role in this case. The paradigmatic third-party cases involve law enforcement agents attempting to obtain data *from third parties*, such as banks or telecommunications companies, about target individuals who have voluntarily disclosed data to those third parties. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735, 737 (1979). Here, by contrast, the CTA compels disclosure of information not from third parties but directly from the target individual or

entity itself. *See Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527 (7th Cir. 2018) (doctrine did not apply when "[t]here is no third party involved . . . ").

Nor is it true that all of the information that the CTA demands is already disclosed elsewhere. The government may be able to obtain from other sources (1) a publicly available list of all of the corporate entities registered in a particular state and (2) a list of all passport numbers that have been issued to any U.S. citizen. But the CTA compels self-reporting of the *relationship* between those two categories of information. And that is the whole point of the CTA. As the government has insisted, without the CTA, federal law enforcement agencies will be unable to close the gap and will be unable to link specific individuals to specific entities. That alone demonstrates both that the relevant information has not actually been disclosed to any third party and that the plaintiffs reasonably expect it to remain private. *See Patel v. City of Los Angeles*, 738 F.3d 1058, 1062 (9th Cir. 2013) ("[I]f the records were publicly accessible, the police of course would not need to rely on [the ordinance] to gain access to them.").

Tax returns do not reveal all individuals who may have "substantial control" over an entity, either. Some of those individuals may not have a formal economic interest in the entity. In other cases, a corporation's shareholders may comprise other corporations, such that its tax filings do not disclose the identity of individuals. In no event, moreover, does an entity expect that its records or ownership information will be provided to foreign intelligence services without court oversight, as the CTA permits. 31 U.S.C. § 5336(c)(2)(B)(ii). In fact,

even federal prosecutors ordinarily may not obtain tax return information from the IRS for use in criminal investigations unless they first obtain a court order from a federal judge. *See* 26 U.S.C. § 6103(i)(1)(A).

B. The Government Failed to Demonstrate That Any Exception to the Warrant Requirement Applies.

Despite acknowledging that the CTA effects a Fourth Amendment search, the Eleventh Circuit pivoted directly to *Shultz* instead of identifying any recognized exception to the warrant requirement. But "searches conducted outside the judicial process, without prior approval by a judge or a magistrate judge, are *per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions." *Patel*, 576 U.S. at 419-20 (cleaned up). "This rule applies to commercial premises as well as to homes." *Id.* (quotation omitted). And *Shultz* is not on any list of the "specifically established" or "well-delineated" exceptions to the warrant requirement. *Id.* at 419; *see also Chandler v. Miller*, 520 U.S. 305, 309 (1997) (exceptions must be narrowly construed).

The Eleventh Circuit skipped the required analysis for a simple reason: none of the acknowledged exceptions to the warrant requirement apply. The primary exception that the government has relied on in other CTA lawsuits is the "closely guarded" special needs exception (otherwise known as the administrative search exception). *Chandler*, 520 U.S. at 309. This exception applies only when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Skinner v. Ry. Lab. Executives' Ass'n*, 489 U.S. 602, 619 (1989). The purpose behind the search is key. Even if a check-

point program is operated in a uniform and nondiscretionary manner, this Court has "never approved a checkpoint program whose primary purpose [is] to detect evidence of ordinary criminal wrongdoing." *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000).

That rule dooms any attempt to fit the CTA into the "special needs" exception. The sole justification for the CTA is the "normal need for law enforcement": namely, to obtain information helpful for criminal prosecution. *Skinner*, 489 U.S. at 619. The government has repeatedly asserted that the CTA was intended to fill a gap in its ability to detect and prosecute financial crime. The disclosure must be made directly to the "Financial Crimes Enforcement Network." 31 U.S.C. § 5336(a)(5), (b)(1)(A). And the purpose of collecting individuals' "sensitive" data under the CTA is solely to build a financial-intelligence database that law enforcement agencies may access to aid their criminal investigations. 31 U.S.C. § 5336 note (6).

Because the express purpose of the CTA is to assist ordinary criminal law enforcement, the "special needs" doctrine does not apply. *Ferguson v. City of Charleston*, 532 U.S. 67, 80 (2001). Whenever a statute authorizes searches "primarily for the ordinary enterprise of investigating crimes," then either a warrant or —at minimum—individualized suspicion is necessary. *Edmond*, 531 U.S. at 44. Even if a search begins as an administrative search, once officers begin to "search[ ] for evidence of crime," they need a warrant. *Michigan v. Tyler*, 436 U.S. 499, 512 (1978). Under the CTA, however, there is no administrative search; officers are searching for evidence of crime from the beginning.

The CTA lacks the other hallmarks of a permissible administrative search, too. To begin with, the doctrine

applies only to certain "pervasively regulated" industries. *Id.* at 424. An industry is pervasively regulated if it has "such a history of government oversight that no reasonable expectation of privacy could exist." *Free Speech Coalition*, 825 F.3d at 169. This Court has applied this "narrow exception" to only four industries: "liquor sales"; "firearms dealing"; "mining"; and "running an automobile junkyard." *Patel*, 576 U.S. at 424. The CTA, by contrast, is not limited to any industry—pervasively regulated or not.

Moreover, "in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain pre-compliance review before a neutral decisionmaker." *Patel*, 576 U.S. at 420; *see also Heidi Grp., Inc. v. Texas Health & Hum. Servs. Comm'n*, 138 F.4th 920, 933 (5th Cir. 2025) ("[T]he government must usually obtain a subpoena before accessing a corporation's books and records."). The CTA not only compels disclosure without any court oversight, but it then allows FinCEN to share that coerced information with virtually any law enforcement agency that asks for it, including foreign governments and intelligence services—all without court oversight or neutral review. 31 U.S.C. § 5336(c)(2)(B)(ii).

C. *Shultz* Does Not Rescue the CTA.

Because no recognized exception to the warrant requirement applies, the warrantless searches compelled by the CTA are unconstitutional. *See, e.g.*, *Patel*, 576 U.S. at 423 (facially invalidating hotel-registry-disclosure ordinance where government could not demonstrate that administrative search exception applied); *Free Speech Coalition*, 825 F.3d at 171, 173 (same analysis); *Airbnb*, 373 F. Supp. 3d at 495 (same analysis).

But even if *Shultz* could function as a stand-in for a warrant exception, it does not apply.

1. *Shultz* Does Not Broadly Authorize Reporting Requirements.

The Eleventh Circuit held that *Shultz* created a special rule for "uniform reporting requirements" that deviates from the strictures that the Fourth Amendment imposes on every other type of search. App.19.

But *Shultz* never purported to announce a universal rule. The majority opinion in *Shultz* upheld only the narrow regulations that had been adopted in order to implement the Bank Secrecy Act; it declined to opine on the constitutionality of the statutory language itself, which allowed the Secretary of the Treasury to impose much broader reporting requirements than he had chosen to impose under the regulations. *Shultz*, 416 U.S. at 63-64. Two of the six-justice majority in *Shultz* —Justices Powell and Blackmun—joined a concurrence observing that, although they agreed that the regulations as issued did not violate the Fourth Amendment, "[a] significant extension of the regulations' reporting requirements . . . would pose substantial and difficult constitutional questions" for them. *Shultz*, 416 U.S. at 78 (Powell, J., and Blackmun, J., concurring).

In fact, *Shultz* never even addressed the Fourth Amendment claims of the individual depositors—that is, the persons whose information was required to be disclosed. Those claims were rejected for lack of standing. *See Shultz*, 416 U.S. at 68-69. And when this Court reviewed the depositors' Fourth Amendment challenges to the Bank Secrecy Act on the merits in *Miller*, the Court rejected those challenges under the third-party doctrine. *Miller*, 425 U.S. at 443. *Shultz*

never purports to control all Fourth Amendment aspects implicated by "reporting requirements."

Nor is there any support for the notion that the Fourth Amendment distinguishes between the forcible disclosure of data in physical form and the forcible disclosure of the same information in electronic form. *Patel* forecloses Congress's ability to compel everyone in America to compile a list on notebook paper of every entity over which they have "substantial control" and make that list available to law enforcement officers who knock on the door and demand it. *See Patel*, 576 U.S. at 420-21. Congress cannot end-run that rule by forcing everyone to mail the same list directly to the FBI's local field office. And because those sorts of physical disclosures violate the Fourth Amendment, the CTA does, too. The information obtained is identical; whether the statute compels the information to be disclosed electronically or in hard copy does not matter. *See Airbnb*, 373 F. Supp. 3d at 495 (discussing forcible disclosure of electronic data).

2. *Shultz* Does Not Permit Suspicionless Searches as Long as They Are Nondiscretionary and "Limited."

Beyond converting *Shultz* into a stand-alone exception to the warrant requirement, the Eleventh Circuit extrapolated from it the wrong lessons. The Eleventh Circuit reasoned that *Shultz* approves of any "reporting requirement" as long as it imposes (1) uniform, nondiscretionary searches that (2) compel the production of purportedly "limited" information. That approach is wrong on both counts.

First, although preventing arbitrary and discretionary searches was one reason why the Framers adopted

the Fourth Amendment, an equally "central aim of the Framers was to place obstacles in the way of a too permeating police surveillance." *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (internal quotation marks and citation omitted). The Eleventh Circuit's analysis fails to acknowledge this second objective of the Fourth Amendment. The Fourth Amendment protects against *unreasonable* intrusions, not merely against *discretionary* intrusions. U.S. Const., amend. IV. A search that would be unreasonably intrusive when applied to a particular individual is not transformed into a Fourth-Amendment-compliant search merely because that same level of unreasonable intrusion is applied to everyone. *Carpenter*, 585 U.S. at 305.

That is why it did not matter in *Edmond* that "the officers have no discretion to stop any vehicle out of sequence." *Edmond*, 531 U.S. at 35. What made the searches unreasonable was not that they were subject to abuse on a case-by-case basis but that they were suspicionless searches whose primary purpose was crime control. *Id.* at 40. The Court refused "to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends." *Id.* at 43. That is because, if officers were permitted to make uniform, discretionless traffic stops for criminal-law enforcement purposes, then there would be nothing to stop officers from subjecting innocent citizens to suspicionless stops as "a routine part of American life," as long as the stops were universal or otherwise without discretion. *Edmond*, 531 U.S. at 42.

In other words, there is no Big Brother exception to the Fourth Amendment. Applying a search regime universally and uniformly does not convert an unrea-

sonable search into a reasonable one. *Id.*; *see also id.* at 56 (Thomas, J., dissenting) ("I rather doubt that the Framers of the Fourth Amendment would have considered 'reasonable' a program of indiscriminate stops of individuals not suspected of wrongdoing."). The Eleventh Circuit has improperly allowed the CTA to do precisely what *Edmond* prohibited, enabling the government to extract private information from innocent citizens without suspicion of wrongdoing, as long as the searches are universal. That holding interprets *Shultz* as enabling an outcome that this Court has repeatedly refused to allow.

Second, it does not help the government's position to insist that the CTA's compelled disclosures are relatively "limited." That argument is like saying that, if the police break into a filing cabinet without a warrant, they do not violate the Fourth Amendment as long as they take out only the one or two pieces of paper that they want. That has never been the rule. Criminal investigators do not have the right to obtain just a little bit of private information in violation of the Fourth Amendment, as long as they leave most of it behind.

To the extent that the Eleventh Circuit believed that the CTA's reporting requirement imposes minimal burden on those who are required to upload the information, the burden of compliance is not the relevant inquiry. Even if technology allows a search to be conducted with little to no effort from the target individual, it still violates the Fourth Amendment if there is an excessive degree of government intrusion into property or privacy interests. That is why searches of cell-site data and thermal imaging are unconstitutional, even though those searches do not require the targeted individuals to engage in any effort at all. *See, e.g.*,

Carpenter, 585 U.S. at 313 (cell-site data); *Kyllo v. United States*, 533 U.S. 27, 35 (2001) (thermal imaging). The relevant question is not whether the search requires effort by the individual being searched; it is whether the search intrudes upon the person's property or privacy interests. *Carpenter*, 585 U.S. at 313; *see also Airbnb*, 373 F. Supp. 3d at 495. And here, the CTA unmistakably does.

3. The Disclosure Regime in *Shultz* Was Much Narrower than the Disclosure Regime Mandated by the CTA.

Even to the extent that *Shultz* suggests that some reporting regimes may be narrowly tailored enough to comply with the Fourth Amendment, the regime at issue in *Shultz* was far different than that imposed by the CTA. *See SBAM*, 769 F. Supp. 3d at 733-37.

a. *Shultz* Compelled Disclosure Only of Transactions That Were Suspicious.

Unlike the CTA, the regulations at issue in *Shultz* compelled disclosure only when there was already a level of individualized suspicion. Under the regulations, banks were required to disclose information only about certain specific, "abnormally large" transactions: namely, transfers of at least $10,000 in currency. *Shultz*, 416 U.S. at 67; *see also id.* at 41 n.14. In fact, the regulations exempted banks from disclosing even those large-currency transfers when they involved "established customer[s]" who maintained accounts consistent with "customary" industry practices. *Id.* at 39.

The Bank Secrecy Act regulations therefore were triggered under circumstances that—like in a valid *Terry* stop—give rise to at least a reasonable suspicion

of illegality. Just as the officers in *Terry* had reasonable suspicion that the suspects' abnormal activity (walking back and forth in front of a store) was a marker of potential criminality, so the anomalous behavior of a brand-new banking customer transferring at least $10,000 in currency gave the government enough suspicion to conduct a limited search that is no more than sufficient to allay the suspicion. *Terry v. Ohio*, 392 U.S. 1, 22-23 (1968). By linking the searches to specific transactions, *Shultz* approved searches that were tied to specific, suspicious circumstances, just like in *Terry*. That is consistent with the general rule that searches and seizures may be effected even for "general crime control purposes" as long as they are based on "some quantum of individualized suspicion." *Ashcroft v. al-Kidd*, 563 U.S. 731, 737-38 (2011).

The CTA is far different. While *Shultz* opined that there must be "a tenable congressional determination as to improper use of transactions of that type in interstate commerce," *Shultz*, 416 U.S. at 67, the CTA is not tied to any "transactions" of any type, suspicious or otherwise. The CTA regulates every small business in America, simply because they exist, not because of anything they do. Unlike the Bank Secrecy Act, the CTA is not targeted at obtaining more information about particular suspicious activity in order to allay the government's legitimate concerns about that activity.

The CTA, instead, creates a database of everyone's information without any antecedent suspicion, merely because an entity has been created. The mere creation of an entity is not "abnormal" or suspicious. The whole purpose of the CTA is simply to create a haystack so that the government can search through it for anything that might look like a needle. That is the same sort of

rummaging that has been anathema to the Fourth Amendment since its adoption. *See Byrd*, 584 U.S. at 403; *Marshall*, 436 U.S. at 311-12. Because *Shultz* involved the constitutionality of searches that *were* supported by some indicia of suspicion, it says very little about the constitutionality of searches under the CTA, which are not.

b. The Disclosures Compelled in *Shultz* Were Much More Limited Than the Disclosures Compelled by the CTA.

The Eleventh Circuit was also wrong to equate the disclosures at issue in *Shultz* with the disclosures at issue here. Exposing the identity of individuals who can control a company or own convertible notes or other contingent interests in it is an intrusive inquiry, not a "limited" one. The government has argued both that the information compelled by the CTA is incredibly minimal but that the government also desperately needs it to fill the "gap" in its law enforcement efforts. The government is arguing both that the information is crucially important and that it has no real value. That is not a winning approach.

Nor is it merely a de minimis intrusion for every small business owner across the country to be subject to a costly and ongoing reporting requirement, under which their private business information may be provided to foreign intelligence agencies. Paying anywhere between $85 to $2,600 in order to hand over information to government actors so that they can prosecute you with it or share it with foreign intelligence services is not the sort of "limited" intrusion that *Shultz* had in mind. It is instead, "a broad, grab-everything collection of suspicionless data because some day, some way,

somehow, someone in law enforcement might find it useful." *SBAM*, 769 F. Supp. 3d at 735.

c. *Shultz* Involved Pervasively Regulated Entities.

Shultz also involved disclosure obligations that were imposed upon entities—banks—that are highly regulated. *Shultz* is therefore best understood as a particular species of administrative search that allows the government to require already-heavily regulated entities to disclose objectively suspicious transactions, not as providing permission for the government to impose suspicionless disclosure obligations on every individual and entity in the country.

Not only did *Shultz* adopt a test that is a close cousin of the administrative search analysis, but *Shultz* also took pains to emphasize that (1) the reporting requirements applied only to banks, not to individual depositors, and (2) banks had been required to furnish these reports for the previous two decades under prior regulatory regimes. *Shultz*, 416 U.S. at 38 & n.12. In other words, the Bank Secrecy Act's reporting requirements applied solely to financial entities that were already pervasively regulated and had already been subject to very similar reporting requirements under other regimes for more than twenty years. That is a hallmark of the administrative search exception. *See Free Speech Coalition*, 825 F.3d at 169-70. It also means that the scope of the Bank Secrecy Act's compelled disclosures is far more limited than the scope of the compelled disclosures under the CTA, which apply to almost every small business in every industry in the country.

II. The Eleventh Circuit's Holding Will Have Profound Effects If It Is Not Corrected.

A. The Eleventh Circuit's Anemic View of the Fourth Amendment Will Fundamentally Change How Law Enforcement Agencies Can Investigate and Prosecute U.S. Citizens.

The Eleventh Circuit did not attempt to reconcile *Shultz* with any of this Court's subsequent Fourth Amendment jurisprudence. Instead, under the Eleventh Circuit's approach, as long as Congress characterizes a search as a "reporting requirement," it can forcibly compel disclosure of information for criminal investigation purposes whenever it determines that this information would be useful to look through in order to determine whether ordinary, unsuspicious citizens were committing crimes.

If *Shultz* applies wholesale to reporting regimes that expressly demand information for criminal law enforcement purposes, the implications will be staggering. In the Eleventh Circuit's view, *Shultz* eliminates not only all of the ordinary Fourth Amendment protections (including individualized suspicion and a warrant) but also all of the protections that would apply to an administrative search (including pre-compliance review, a non-law-enforcement purpose, and application only to pervasively regulated industries). Congress—or State and local government actors—could sidestep the Fourth Amendment and provide law enforcement officers with suspicionless access to private information as long as they enacted discretionless "reporting regimes" instead of spot-check inspections. *See Airbnb*, 373 F. Supp. 3d at 491, 495 (noting implications of such a regime).

The pace of technological advancement simply raises the stakes. In the age of big data and artificial intelligence, the significantly reduced cost of administering and searching large databases make it vastly more tempting for government actors to collect and cross-index as much data on citizens as they can. *See Airbnb*, 373 F. Supp. 3d at 491, 495 (noting implications of such a regime); *see also SBAM*, 769 F. Supp. 3d at 732 n.6. Upholding the CTA allows governments to compel Americans to actively contribute nonpublic information to the dossier that law enforcement agencies already have on file for them—all without any suspicion that any one in particular has done anything wrong. That sort of investigatory regime would be permissible only under a far different conception of the Fourth Amendment than the one that the Framers adopted. *United States v. Di Re*, 332 U.S. 581, 595 (1948); *see also Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

This result is even more troubling because circumventing the Fourth Amendment is exactly what Congress enacted the CTA to do. FinCEN's then-Director testified to Congress that the CTA would be helpful for law enforcement because it would eliminate investigators' need to comply with the ordinary tools of investigation—like "grand jury subpoenas" and "search warrants"—to obtain beneficial ownership information. 87 Fed. Reg. at 59504. According to the Director, complying with these requirements "takes an enormous amount of time" and "wastes resources." *Id.* Grand jury subpoenas, for example, were insufficient because they "require an underlying grand jury investigation into a possible violation of law." *Id.* The CTA was designed to make ownership information "immediately available to law enforcement, intelligence, or national

security agencies" without the hassle of a warrant or judicial oversight. *Id*. at 59505. The Eleventh Circuit's approval of the CTA rewards its intentional end-run around the Constitution.

B. Allowing the Government to Force Private Information from U.S. Citizens So That They Can Be Prosecuted with It Is an Invitation for Abuse.

The Eleventh Circuit downplayed the dangers inherent in providing governments the power to collect data on citizens for criminal law-enforcement purposes without any antecedent suspicion, reasoning that "periodic audits" by other executive-branch members would ensure that FinCEN does not use inappropriately use or share the data it squeezes out of citizens under the CTA. App.20. That optimism is unwarranted.

First, despite the Eleventh Circuit's attempts to minimize the degree to which information can be shared under the CTA, the statute in fact expressly permits data extracted by the statute from U.S. citizens to be shared with any prosecutor who asks for it, *see* 31 U.S.C. § 5336(c)(2)(B)(i)(II), and even with "law enforcement . . . or prosecutorial authorities" in "trusted foreign countries" at their request and at the executive branch's discretion, *see* 31 U.S.C. § 5336(c) (2)(B)(ii). Nothing in the statute prevents the executive branch from sharing with prosecutors and foreign intelligence agencies private data that it compelled a public servant or potential political rival to disclose under the CTA.

Second, events both past and present expose the hollowness of the lower court's confidence that misuse of CTA-compelled data would be adequately deterred by "periodic audits" conducted by other officials within

the executive branch. Government actors have an unfortunate history of misusing data that they collect about law-abiding citizens.[5] The FBI, for example, illegally accessed a government database "more than 278,000 times" over the course of several years, "including searching for communications of people arrested at protests of police violence and people who donated to a congressional candidate."[6] The IRS recently agreed to share certain taxpayer data with DHS so that DHS could pursue immigration and potential criminal investigations.[7] Allegations have swirled that rogue actors have misused data to which they had access in their governmental capacities.[8] And intentional misuse of private data is only one part of the problem. Infor-

---

[5] *See* Stephanie K. Pell, et al., *Privacy under siege: DOGE's one big, beautiful database*, Brookings Institution (June 25, 2025), https://www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/ (discussing impetus for federal Privacy Act).

[6] Electronic Frontier Foundation, *Newly Public FISC Opinion is The Best Evidence For Why Congress Must End Section 702* (May 23, 2023), https://www.eff.org/deeplinks/2023/05/newly-public-fisc-opinion-best-evidence-why-congress-must-end-section-702.

[7] *See* Bogage, Jacob *et al.*, *IRS improperly disclosed confidential immigrant tax data to DHS*, THE WASHINGTON POST (Feb. 11, 2026), https://www.washingtonpost.com/business/2026/02/11/immigrants-irs-dhs-tax-data/.

[8] *See, e.g.*, Kornfield, Meryl, et al., *Whistleblower claims ex-DOGE member says he took Social Security data to new job*, THE WASHINGTON POST (Mar. 10, 2026), https://www.washingtonpost.com/politics/2026/03/10/social-security-data-breach-doge-2/(Social Security Administration investigating a claim by a former U.S. DOGE Service employee that "he had access to two highly sensitive agency databases and planned to share the information with his private employer").

mation collected by government agencies may also be improperly shared through carelessness or mistake.[9]

The mass data collection embodied in the CTA only exacerbates these risks. And in the meantime, the statute tramples Americans' civil liberties "at a cost of billions of dollars to the citizens least likely to afford it." *SBAM*, 769 F. Supp. 3d at 739. The Fourth Amendment was designed to prevent the government from squeezing information from law-abiding citizens for criminal-investigation purposes without any suspicion of wrongdoing. Forcing American citizens to pay for the panopticon simply adds insult to injury.

---

[9] *See* Kanno-Youngs, Zolan and Sanger, David E., *Border Agency's Images of Travelers Stolen in Hack*, N.Y. TIMES (Jun. 10, 2019), https://www.nytimes.com/2019/06/10/us/politics/customs-data-breach.html (federal subcontractor improperly transferred "tens of thousands of images of travelers and license plates" stored by CPB, which were later hacked); Greenberg, Andy, *The Year of the Mega Data Breach*, FORBES (Nov. 24, 2009), https://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches.html (the National Records Association sent a hard drive with the personal information of 76 million servicemembers to an IT contractor without wiping the data).

CONCLUSION

The petition should be granted.

Respectfully submitted,

Stephen J. van Stempvoort
Counsel of Record
D. Andrew Portinga
Amanda L. Rauh-Bieri
MILLER JOHNSON
45 Ottawa Avenue SW, Suite 1100
Grand Rapids, MI 49503
(616) 831-1700
vanstempvoorts@millerjohnson.com

Counsel for Amici Curiae

May 21, 2026