No. 24-40792

United States Court of Appeals for the Fifth Circuit

TEXAS TOP COP SHOP, INCORPORATED; RUSSELL STRAAYER; MUSTARDSEED LIVESTOCK, L.L.C.; LIBERTARIAN PARTY OF MISSISSIPPI; NATIONAL FEDERATION OF INDEPENDENT BUSINESS, INCORPORATED; DATA COMM FOR BUSINESS, INCORPORATED,

Plaintiffs-Appellees,

v.

MERRICK GARLAND, U.S. ATTORNEY GENERAL; TREASURY DEPARTMENT; DIRECTOR FINCEN ANDREA GACKI, DIRECTOR OF THE FINANCIAL CRIMES ENFORCEMENT NETWORK; FINANCIAL CRIMES ENFORCEMENT NETWORK; JANET YELLEN, SECRETARY, U.S. DEPARTMENT OF TREASURY,

Defendants-Appellants,

On Appeal from the United States District Court
for the Eastern District of Texas
No. 4:24-cv-478, Hon. Amos L. Mazzant

BRIEF FOR *AMICUS CURIAE* PROJECT FOR PRIVACY AND SURVEILLANCE ACCOUNTABILITY, INC. IN SUPPORT OF APPELLEES AND IN OPPOSITION TO APPELLANTS' EMERGENCY MOTION FOR STAY PENDING APPEAL

Gene C. Schaerr
Counsel of Record
Erik S. Jaffe
Brian J. Field
Aaron C. Ward
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae Project for Privacy and Surveillance Accountability, Inc.

DECEMBER 18, 2024

SUPPLEMENTAL STATEMENT OF INTERESTED PERSONS

No. 24-40792
Texas Top Cop Shop, et al. v. Garland, et al.

Pursuant to 5th Cir. R. 29.2, the undersigned counsel of record hereby certifies that, in addition to the persons and entities listed in the Appellants' and Appellees' Certificates of Interested Persons, the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

Amicus Curiae:
Project for Privacy and Surveillance Accountability, Inc.

Counsel for *Amicus Curiae*:
Gene C. Schaerr
Erik S. Jaffe
Brian J. Field
Aaron C. Ward
SCHAERR | JAFFE LLP

In accordance with Federal Rule of Appellate Procedure 26.1, *amicus curiae* Project for Privacy and Surveillance Accountability, Inc. states that it is not publicly traded and has no parent corporations. No publicly traded corporation owns 10% or more of *amicus*.

/s/ Gene C. Schaerr
Gene C. Schaerr
Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Constitutional Provision

Statutes

Rule

Treatise

Other Authorities

IDENTITY AND INTEREST OF *AMICUS CURIAE*[1] AND SOURCE OF AUTHORITY TO FILE BRIEF

Beyond exceeding the government's authority, the Corporate Transparency Act ("CTA" or "the Act") also violates the Fourth Amendment because collecting and compiling the data required by the CTA and using such compilation for law enforcement constitutes a warrantless search lacking probable cause or even reasonable suspicion. *Amicus* agrees with Plaintiffs/Appellees that the CTA's *disclosure* requirements are overly intrusive and well beyond the historical norm of reporting corporate officers and directors to a state government. *Amicus* would add that the CTA's *database* provisions are even more disturbing. Sensitive information obtained from the Act's sweeping disclosure requirements are compiled into a database that can be accessed by "Federal, State, and Tribal" authorities without any judicial oversight. *See* 31 U.S.C. § 5336(d)(2).

---

[1] This brief is accompanied by a motion for leave to file and all parties have consented to its filing. No party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund the preparation or submission of the brief, and no person other than *amicus*, its members, or its counsel contributed money to fund the preparation or submission of the brief. Fed. R. App. P. 29(a)(4)(E).

Because of the serious privacy issues they raise, the CTA's database provisions are of particular concern to *Amicus Curiae* Project for Privacy and Surveillance Accountability, Inc. ("PPSA"), a nonprofit, nonpartisan organization dedicated to protecting privacy rights and guarding against an expansive surveillance state. *Amicus* PPSA files this brief to urge this Court to deny defendants' motion for a stay pending appeal because the Fourth Amendment is an additional or alternative ground for agreeing with Appellees' likelihood of success on the merits and strengthens the public interest in maintaining the injunction.

SUMMARY OF ARGUMENT

The Fourth Amendment ensures a Founding-era level of privacy despite technological advances. *Carpenter v. United* States, 585 U.S. 296, 305 (2018). The CTA intrudes upon that privacy by requiring beneficial owners to disclose personal information on an ongoing basis for use in a comprehensive "database for beneficial ownership information" to be used by Treasury and other government agencies. 31 U.S.C. §§ 5336(d)(2), (b)(2)(A), (b)(1)(D).

Because of the database provision, such disclosures must be evaluated under the Supreme Court's high-tech surveillance precedent.

See Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 345 (4th Cir. 2021). Given the risk of abuse—particularly against ideological or non-profit corporations—such widespread data collection certainly constitutes a "search" for Fourth Amendment purposes. And the attendant risks will only grow worse with advances in artificial intelligence and data analysis technology.

Such searches, without a warrant based on probable cause, are unreasonable and do not fall under any explicitly delineated exception to the warrant requirement. *See Colorado v. Bannister*, 449 U.S. 1, 2–3 (1980). And they cannot be justified as part of longstanding income tax collection practices. *See California Bankers Ass'n v. Shultz*, 416 U.S. 21, 60 (1974).

Plaintiffs are likely to succeed on the merits, the public interest favors avoiding unconstitutional data compilation, and there would be irreparable harm to other parties if the preliminary injunction is lifted. The motion for a stay pending appeal should be denied.

ARGUMENT

The Fourth Amendment provides that Americans have the right to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. Const. amend. IV. That Amendment is designed to ensure that Americans enjoy a level of privacy at least equal to the privacy expectations that existed during the Founding era. The Amendment should therefore be understood to "safeguard the privacy and security of individuals against arbitrary invasions by governmental officials" to a similar level. *Carpenter*, 585 U.S. at 303–04.

But the CTA requires, *inter alia*, extensive reporting of beneficial owners' personal identifying information, with perpetual obligations to update such information. 31 U.S.C. §§ 5336(b)(2)(A), (b)(1)(D). All that information mut be stored in an "accurate, complete, and highly useful database for beneficial ownership information" to be used in conjunction with "Federal, State, and Tribal" authorities, and can apparently be queried by those authorities at will. *Id.* § 5336(d).

These reporting and database requirements do not require a warrant based on probable cause and thus constitute unreasonable

Fourth Amendment searches because their potential for abuse is incompatible with Founding-era expectations of privacy. *Carpenter*, 585 U.S. at 320 (discussing the threat posed by comprehensive databases).

I. Disclosure Requirements for Subsequent Use in a Database Are Fourth Amendment Searches.

A Fourth Amendment search occurs when information or items are seized, the person has a subjective expectation of privacy in the information or items seized, and the expectation would have been recognized as reasonable at the time of the Founding. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Carpenter*, 585 U.S. at 305; *United States v. Smith*, 110 F.4th 817, 831 (5th Cir. 2024). Here, the required disclosures, and their subsequent incorporation into a database, violate both subjective and objective expectations of privacy, and thus constitute searches.

A. Beneficial owners easily clear the low bar for a subjective expectation of privacy.

A subjective expectation of privacy exists when an individual "has shown that he seeks to preserve something as private." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (cleaned up). It is such a low bar that it "is not frequently litigated." 3A Charles A. Wright & Arthur R. Miller, *Federal Practice & Procedure* § 663 (4th ed. 2023 update) (Scope of

Fourth Amendment—Definition of Search). Even a "burglar plying his trade in a summer cabin during the off season may have a thoroughly justified *subjective* expectation of privacy[.]" *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (emphasis added).

That the information at issue was generally kept private prior to disclosure suffices to demonstrate a subjective expectation of privacy. *Patel v. City of Los Angeles*, 738 F.3d 1058, 1062 (9th Cir. 2013) ("We do not believe business owners are required to prove that proposition, any more than homeowners are required to prove that papers stored in a desk drawer are subject to a reasonable expectation of privacy."), *aff'd*, 576 U.S. 409 (2015).

B. The expectation of privacy is objectively reasonable.

In determining whether disclosure requirements constitute a search, the Court also considers how the disclosed information will be used in a database or "in combination with other information[.]" *Carpenter*, 585 U.S. at 312; *Smith,* 110 F.4th at 834 n.8 ("In *Carpenter* ... The question was whether the technology utilized by law enforcement had the *capability* of providing data that offered 'an all-encompassing record of [a person's] whereabouts,'" (quoting *Carpenter,* 585 U.S. at 311)

(emphasis in original)); *Leaders of a Beautiful Struggle,* 2 F.4th at 345. And, when the database is sophisticated or comprehensive, as it is here, courts should apply the Fourth Amendment test associated with high-tech surveillance techniques. *See, e.g.*, *Smith*, 110 F.4th at 832 (noting heightened privacy concerns from an "exhaustive chronicle of [] information" (quoting *Carpenter*, 585 U.S. at 314)); *Leaders of a Beautiful Struggle*, 2 F.4th at 341, 345 ("*Carpenter* applies squarely to" a case involving "creation of a retrospective database"); *Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1101 (Mass. 2020) (applying *Carpenter* and analogous state-law test because data was collected for use in large database); 31 U.S.C. § 5336(d)(2) (database provision).

Carpenter explained that courts should consider (1) the amount and intimacy of information collected, (2) the number of people surveilled, (3) inescapability of the surveillance, (4) whether there is automatic disclosure of information, and (5) the cost of the surveillance. Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 Harv. L. Rev. 1790, 1800 (2022). And here, all five *Carpenter* factors show that the CTA's collection for database usage constitutes a search.

1. The CTA's collections for use in a database easily implicate the first *Carpenter* factor because financial surveillance, like geofence data this Court recently addressed, "has the capability of revealing intimate, private details about a person's life, thus conferring a 'reasonable expectation of privacy.'" *Smith*, 110 F.4th at 834 n.8 (quoting *Carpenter*, 585 U.S. at 311).

This is a particular danger for (c)(4) corporations designed to facilitate non-profit associations or for-profit entities with an ideological focus—such as dealers in controversial political literature or other expressive entities. Much like with membership in a tax-exempt organization, disclosing this information could subject the beneficial owners to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *NAACP v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958).

Disclosure of such information also could subject beneficial owners to retaliatory investigations, a real concern given the history of politically-tinged investigations by the Department and other federal agencies. For instance, the Department entity at issue here—known as the Financial Crimes Enforcement Network or FINCEN—has

encouraged banks to comb through transactions involving sporting goods stores such as Cabela's to identify "extremists," and other agencies have urged flagging purchases associated with major political candidates. *See* Staff of H. Comm. on Judiciary & Select Subcomm. on the Weaponization of the Fed. Gov't, *Financial Surveillance In The United States: How Federal Law Enforcement Commandeered Financial Institutions To Spy On Americans* 2–3 (Mar. 6, 2024), https://tinyurl.com/3atzt7cd. Even if it does not occur in every case, the capability for such misuse is enough to create an expectation of privacy. *See Smith*, 110 F.4th at 834 n.8 ("This is general inquiry, not a retroactive, *post-hoc* examination based on the *results* of the search in our case" (emphasis in original)).

Beyond the present threat, information collection for database usage must be evaluated in light of foreseeable future technology, including rapidly advancing artificial intelligence. "[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" *Carpenter,* 585 U.S. at 313 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)); *Smith*, 110 F.4th at 841 (Ho, J., concurring) ("modern technology has proven to be a blessing as well as a curse. Our panel decision today endeavors to apply our Founding charter

to the realities of modern technology, consistent with governing precedent.").

As early as the 1970s, it was known that financial surveillance "can reveal much about a person's activities, associations, and beliefs." *Shultz*, 416 U.S. at 78–79 (Powell, J., concurring). But "modern technology tends to produce databases of telephone or financial information that are far more voluminous and detailed than the records at issue in those 1970s cases[.]" Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. 357, 381 (2019). The ability to aggregate information from multiple databases enhances the utility of the data, making it more revealing than when considered individually. *See* Andrew Guthrie Ferguson*, Persistent Surveillance*, 74 Ala. L. Rev. 1, 47–48 (2022).

For example, even now, machine learning methods can detect consistent authors from a few anonymous writings. *See* Ahmed Abbasi et al., *Authorship Identification Using Ensemble Learning,* 12 Sci. Reps. 9537 (2022). It is easy to foresee a scenario where an agency dislikes views expressed in anonymous social media posts, identifies the author, looks for any businesses where the author has beneficial ownership, and "flags" that business for review to banks. And the privacy problems will

only become worse as increasingly sophisticated AI systems are able to analyze "in the aggregate these millions of data points" to find intimate personal details from large databases. Emily Nicolella, *Evolving Privacy Protections for Emerging Machine Learning Data Under* Carpenter v. United States, 17 FIU L. Rev. 453, 474 (2023).

2. The other *Carpenter* factors also support this conclusion. As to the second, the CTA collects private information from millions or tens of millions of businesses. Third, such collection is inescapable and effectively automatic due to its being legally mandated—with no way to remove one's name from the database even after many years. Finally, collecting such information costs the government no more than processing submitted forms (or running a query into a database), encouraging mass surveillance. *See Smith*, 110 F.4th at 833 (noting danger to privacy posed by ability to collect data "[w]ith 'just the click of a button'" (quoting *Carpenter*, 585 U.S. at 311)).

Thus, there is today a reasonable expectation of privacy against the CTA's collection of financial data for use in a database that can then be queried at will by government enforcement agents.

II. The CTA's Disclosure Requirements for Subsequent Use in a Database Are Unreasonable.

The CTA's data compilation also is unreasonable. It "is axiomatic that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment–subject only to a few specifically established and well delineated exceptions.'" *Bannister*, 449 U.S. at 2–3 (quoting *Katz,* 389 U.S. at 357). The CTA's disclosure requirements do not involve individualized judicial process and a warrant based on probable cause and hence are unreasonable per se.

This lack of process distinguishes the CTA from the regulations at issue in *California Bankers Association v. Shultz*, 416 U.S. 21 (1974). There, "[n]either the provisions [at issue] nor the implementing regulations require[d] that any information contained in the records be disclosed to the Government; both the legislative history and the regulations ma[d]e specific reference to the fact that access to the records is to be controlled by existing legal process." *Id.* at 52.

Nor can the database be justified as a tax collection tool not subject to ordinary Fourth Amendment constraints. This is far from "the ordinary procedure . . . of requiring tax returns to be made," *Flint v. Stone*

Tracy Co., 220 U.S. 107, 175 (1911), *abrogated on other grounds by Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528 (1985), or "the settled practices of the tax collection process[,]" *Shultz*, 416 U.S. at 60. And this is especially true when the program calls for collection and subsequent use in an indefinitely stored database—used in cooperation with agencies that do not even enforce federal tax law. *See* 31 U.S.C. § 5336(d)(2) ("State[] and Tribal" authorities will be involved).

The government also has argued in the alternative that the special needs exemption applies. *See* Br. in Opp'n to Pls.' Mot. for Prelim. Inj. at 28, No. 4:24-cv-00478 (ALM) (E.D. Tex.), ECF No. 18. But the government has conceded that the CTA "generally contemplates that reported information be used to facilitate the investigation and prosecution of financial crimes." *Id.* at 5. And the special needs exception only applies for "concerns other than crime detection[,]" *Chandler v. Miller*, 520 U.S. 305, 313–14 (1997).

Even where the special needs exemption does apply, "courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties." *Chandler,* 520 U.S.

at 314. This exception cannot plausibly apply to millions of beneficial owners on a wholesale basis.

Absent such recognized exceptions, the sweeping searches under the CTA are unreasonable because they lack individualized warrants based on probable cause. The CTA's violation of the Fourth Amendment provides an additional or alternative ground to deny the motion for a stay, which was "supported by the record and presented to the district court." *Amerisure Mut. Ins. Co. v. Arch Specialty Ins. Co.*, 784 F.3d 270, 273 (5th Cir. 2015).

CONCLUSION

The CTA's violation of the Fourth Amendment adds further weight to Plaintiffs' likelihood of success on the merits and to the public interest in maintaining the injunction entered below. This Court should deny the motion for a stay pending appeal.

December 18, 2024

Respectfully submitted,

/s/ Gene C. Schaerr
Gene C. Schaerr
Counsel of Record
Erik S. Jaffe
Brian J. Field
Aaron C. Ward
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
Facsimile: (202) 776-0136
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae
Project for Privacy and
Surveillance Accountability, Inc.

CERTIFICATE OF SERVICE

Pursuant to Fed. R. App. P. 25(d) and 5th Cir. R. 25.2.5, I hereby certify that on December 18, 2024, I filed the foregoing Brief with the Clerk of the Court for the United States Court of Appeals for the Fifth Circuit by using the Court's CM/ECF system; service on counsel for all parties was accomplished by service through the Court's electronic filing system.

/s/ Gene C. Schaerr
Gene C. Schaerr

CERTIFICATE OF COMPLIANCE

The foregoing brief contains 2,589 words excluding the parts of the brief exempted by Fed. R. App. P. 32(f), and complies with the type-volume limitation of Rules 29(a)(5) and 27(d) of the Fed. R. App. P.

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5)(A) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word Office 2016 in 14-point Century Schoolbook font.

December 18, 2024

/s/ Gene C. Schaerr
Gene C. Schaerr