Case No. 24-10736

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

NATIONAL SMALL BUSINESS UNITED, ET AL.,
Plaintiffs-Appellees,
v.
U.S. DEPARTMENT OF TREASURY, ET AL.,
Defendants-Appellees,

Appeal from the United States District Court
for the Northern District of Alabama

No. 5:22-cv-01448-LCB (The Hon. Liles C. Burke)

BRIEF OF *AMICUS CURIAE* HAMILTON LINCOLN LAW INSTITUTE IN SUPPORT OF APPELLEES AND AFFIRMANCE

Neville S. Hedley
HAMILTON LINCOLN LAW INSTITUTE
1629 K Street NW, Suite 300
Washington, DC 20006
(312) 342-6008
ned.hedley@hlli.org
Attorneys for Amicus Curiae

Certificate of Interested Persons and Corporate Disclosures

Under Cir. R. 28-1(b) and Fed. R. App. P. 26.1, I certify that Hamilton Lincoln Law Institute is not a subsidiary or affiliate of a publicly owned corporation and there is no publicly held corporation that owns ten percent or more of any stock issued by him.

Under Cir. R. 28-1(b) and Cir. R. 26.1-2, the following trial judges, attorneys, persons, association of persons, firms, partnerships, and corporations are believed to have an interest in the outcome of this case or appeal:

1. Alabama Property Management, Inc.
2. Bardwell, Will
3. Barger, James Frederick Jr.
4. Boyce, Sean
5. Burke, Liles C., U.S. District Court
6. Boynton, Brian M.
7. Brown, Kenyen
8. Das, Himamauli, former Acting Director of the Financial Crimes Enforcement Network
9. Democracy Forward Foundation
10. Escalona, Prim F., United States Attorney
11. Foundation for Defense of Democracies

12. Gacki, Andrea, Director of the Financial Crimes Enforcement Network
13. Greytak, Scott
14. Hamilton Lincoln Law Institute
15. Hazel, Steven
16. Hedley, Neville S.
17. Healy, Terrence M.
18. Kellerher, Diane
19. Lee, Thomas
20. Loshin, Jacob
21. MacBride, Neil H.
22. McCracken, Todd
23. Miller, Kristen Paige
24. National Small Business United
25. Neiman, John C. Jr.
26. Park, Heeyoung (Linda)
27. Pitz, Taylor
28. Reed, Jack, United States Senator
29. Robinson, Stuart Justin
30. Sibley, Nate
31. Taylor, Jonathan E.
32. Tax Law Center at NYU School of Law
33. Tenny, Daniel

34. Thurston, Robin F.
35. Transparency International
36. United States Department of the Treasury
37. Walthall, James Elliot
38. Warren, Elizabeth, United States Senator
39. Waters, Maxine, United States Representative
40. Whitehouse, Sheldon, United States Senator
41. Winkles, Issac
42. Wyden, Ron, United States Senator
43. Yellen, Janet, Secretary of U.S. Department of the Treasury

Dated: May 20, 2024

/s/ Neville S. Hedley

Neville S. Hedley
HAMILTON LINCOLN LAW INSTITUTE
1629 K Street NW, Suite 300
Washington, DC 20006
Telephone: (312) 342-6008
Email: ned.hedley@hlli.org

Attorneys for Amicus Curia

Table of Contents

Table of Citations

Cases

Rules, Statutes, and Constitutional Provisions

Other Authorities

Interest of Amicus Curiae

Hamilton Lincoln Law Institute ("HLLI") is a public interest organization dedicated to protecting free markets, free speech, limited government, and separation of powers against regulatory abuse and rent-seeking. HLLI, which is independent of the parties to this action, litigates subjects particularly relevant to this case, including Constitutional issues and challenging government overreach and regulatory abuse. *See, e.g.*, *McDonald v. Lawson*, 94 F.4th 864 (9th Cir. 2024) (challenging state law that restricts free speech of physicians, mooted by legislative repeal); *Competitive Enter. Inst. v. FCC*, 970 F.3d 372 (D.C. Cir. 2020) (challenging regulatory action).

HLLI files this amicus brief in support of affirmance of the district court's decision. Counsel for the parties to this appeal have consented to the filing. As FRAP 29(a)(4)(E) requires, HLLI states that no party's counsel authored the brief in whole or in part; and that no person contributed money that was intended to fund preparing or submitting the brief.

Statement of the Issue

Should this Court affirm the district court's judgment and injunction barring enforcement of the Corporate Transparency Act on the alternative ground that the Act violates the Fourth Amendment's prohibition against unreasonable search and seizures?

Summary of Argument

"The constitutional guaranty of the right of the people **to be secure** in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) (emphasis added).

"The Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of security." Jed Rubenfield, *The End of Privacy*, 61 STAN. L. REV.101, 104 (Oct. 2008); *see generally* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security*, 33 WAKE FOREST L. REV. 307 (1998) (arguing that essential language of Fourth Amendment is right of individuals to be secure from unreasonable government intrusion). And recent Supreme Court cases underscore the core principles of the Fourth Amendment and the Framers' intent to limit unchecked government power and secure individual liberty. *See, e.g., Carpenter v. United States*, 585 U.S. 296, 303 (2018) ("The 'basic purpose of this Amendment … is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.'" (quoting *Camara v. Municipal Court of City and Cnty of San Francisco*, 387 U.S. 523, 528 (1967))); *City of Los Angeles v. Patel*, 576 U.S. 409 (2015). The Corporate Transparency Act's ("CTA") compelled disclosure of sensitive personal identification information ("PII") and beneficial ownership information ("BOI"), simply for the act of forming a state-chartered business entity, coupled with the

government's unfettered access to the data stored in a government database specifically for the purpose of conducting criminal investigations is fundamentally at odds with the Fourth Amendment.

This is true even under the "reasonable expectation of privacy" standard. Appellants assert that Appellees have no privacy rights in the data the CTA requires to be disclosed because of previous disclosures to third parties or the data itself does not warrant privacy protections. Both assertions are flawed, and fundamentally misunderstand that the core Fourth Amendment violation is that the statute mandates the disclosure of sensitive information to a government-controlled database—a database which the government may search at will with no notice and no reasonable suspicion of criminal conduct, much less probable cause.

Recent history has demonstrated that the government's unfettered access to sensitive data accumulated and aggregated in bulk is a recipe for abuse and far too akin to the general warrants and writs of assistance that were anathema to the Founders. Thus, the CTA's similarities to the general warrants and writs of assistance are too close for Constitutional comfort.

This Court reviews de novo a district court's ruling on a motion for summary judgment. *SEC v. Almagarby*, 92 F.4th 1306, 1314 (11th Cir. 2024). Although the district court never reached the Fourth Amendment arguments raised below, this Court may consider the Fourth Amendment as an alternative ground for finding in favor of the plaintiff-appellees and

bar enforcement of the CTA. *See Krutzig v. Pulte Home Corp.*, 602 F.3d 1231, 1225 (11th Cir. 2010).

Argument

I. The CTA violates Appellees' Fourth Amendment Rights because it is an unreasonable intrusion by the government. Appellees have a reasonable expectation of privacy in the data and the government's unrestricted ability to search the data exceeds the limits of the Fourth Amendment.

A. The CTA is an unreasonable infringement upon Appellees' security interests.

The Fourth Amendment states that the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. This protection extends "to the orderly taking under compulsion of process" including disclosures compelled by statute or regulation. *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950). "What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile. There he is protected from unwarranted governmental intrusion. And when he puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it

will be secure from an unreasonable search or an unreasonable seizure." *United States v. Hoffa*, 385 U.S. 293, 301 (1966).

The drafters of the Constitution specifically included the Fourth Amendment to address one of the most pernicious practices of the Crown that the Founders found so objectionable—the use of general warrants or writs of assistance. "One thing about which every Fourth Amendment scholar agrees (any there probably is only one such thing) is that the Fourth Amendment was meant to prohibit 'general warrants.'" Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L. REV. 1721 (2014); *see also* Rubenfield, *supra* at 122 ("The Fourth Amendment was enacted above all to forbid 'general warrants.'"). "[T]he original purpose of the Fourth Amendment was not so much privacy as it was to place substantive limitations on the scope of government power" and the guarantee of this right against such power "was central to the ultimate ratification of the Constitution." Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1450 (2017).

General warrants and the similar writs of assistance were excessively broad that "allowed officers to search wherever they wanted and to seize whatever they wanted, with few exceptions." Leonard W. Levy, ORIGINS OF THE BILL OF RIGHTS 153 (1999). The CTA incorporates features of general warrants and writs of assistance that the Founders found so objectionable. The CTA requires a "reporting company" to

disclose the personal information of its "beneficial owners" and "applicants" including legal names, birthdates, current addresses, and identification numbers to FinCEN without any individualized suspicion of wrongdoing. 31 U.S.C. § 5336(b)(1)-(2). The purpose is to allow FinCEN to build a financial-intelligence database that domestic and foreign law enforcement agencies may access to investigate suspected financial crimes. Treasury employees have carte blanche to access the database. 31 U.S.C. § 5336(c)(5).

While the Supreme Court has not had cause to address a statute of such dramatic sweep, its decision in *City of Los Angeles v. Patel,* 576 U.S. 409 (2015) provides the best guidance. That case addressed a city ordinance the required hotels to collect and make available to police on demand a "guest's name and address" and other sensitive information. *Id.* at 412. It further held that facial challenges to statutes authorizing warrantless searches were permissible. *Id.* at 415.

The Court assumed that the ordinance authorized searches for purposes other than for conducting criminal investigations, but still held that the Fourth Amendment warrant requirement applied. 576 U.S. at 420 (subject of even an administrative search "must be afforded an opportunity to obtain pre-compliance review before a neutral decisionmaker"). The CTA transgresses the Fourth Amendment more blatantly than the ordinance in *Patel*. The purpose of the CTA is to

conduct criminal investigations. AOB 6.[1] It compels reporting companies to collect and disclose PII and BOI to FinCEN, and any person who fails to turn over the required information—not just the reporting companies—is subject to penalties. It mandates disclosure even when there is no suspicion of illegal activity, and it allows government agents to search the database at will without a warrant or any opportunity for pre-compliance review before a neutral party. If a non-criminal local ordinance requiring involuntary disclosure of sensitive information fell short of Fourth Amendment requirements, it stands to reason that the CTA also falls short and should not be enforced.

Appellants emphasize that the CTA will make complex investigations less "laborious" and more efficient. AOB 4, 19. But ease and efficiency are not paramount concerns of the Fourth Amendment or our criminal justice system. The state's power to deprive an individual of his liberty is limited not only by the presumption of innocence and the reasonable doubt standard for conviction, but also the right to be free from police monitoring unless there is probable cause that the individual committed a crime. The warrant requirement forces police to persuade a judge that criminality has occurred or is afoot. That might be inconvenient or "laborious," but that is the point. *See Johnson v. United*

[1] References to the Appellants Opening Brief are AOB, and references to filings at the district court are represented as "Dkt. # at _."

States, 333 U.S. 10, 13-14 (1948). More recently, the Court emphasized "that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 585 U.S. at 305 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

The Court's rare approval of mass *ex ante* searches is limited to circumstances not applicable to the broad sweep of the CTA. For instance, in *Illinois v. Lidster* the Court upheld as reasonable a specific instance of mass search and seizure without individualized suspicion or probable cause. 540 U.S. 419, 425-26 (2004). One week after a fatal hit-and-run, police implemented a road checkpoint to solicit public assistance from motorists who regularly traveled that road at the time of the accident. The checkpoint was not "primarily for general crime control purposes, *i.e.*, 'to detect evidence of ordinary criminal wrongdoing.'" *Id.* at 423. (quoting *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000)). Rather, the checkpoint was aimed at investigating a specific crime and "interfered only minimally with liberty of the sort the Fourth Amendment seeks to protect." *Id.* at 427. Those factors weighed in favor of the Court holding the search reasonable. The mandatory disclosure of sensitive data required by the CTA, by contrast, is not targeted at a specific crime—or any crime—and constitutes an unavoidable *ex ante* dragnet sweeping up the sensitive data of all individuals who are associated with the ownership of a state-chartered business entity. That

data then becomes searchable at will by government agents without so much as a showing of reasonable suspicion, never mind probable cause.

The CTA is also distinguishable from government intrusions that are more passive and not intended to be in the realm of criminal enforcement. For instance, in *Naperville Smart Meter Awareness v. City of Naperville,* the Seventh Circuit concluded that a city's mass data collection from smart electricity meters was a search under the Fourth Amendment but deemed it reasonable because there was "no prosecutorial intent." 900 F.3d 521, 528 (7th Cir. 2018). The same cannot be said for the CTA, which Appellants readily concede is intended to be a law enforcement investigative and prosecutorial tool.

B. Appellees have a reasonable expectation of privacy in the data the CTA requires to be disclosed directly to the government, even in instances when there has been limited disclosure to third parties.

1. Appellees have a reasonable expectation of privacy.

The CTA also oversteps the limits imposed by the Fourth Amendment because it does represent an intrusion on the plaintiffs' "reasonable expectation of privacy." *See Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). In the landmark decision of *Boyd v. United States*, the Court acknowledged the importance of privacy interests when it held that "compulsory production of a man's **private**

papers to establish a criminal charge against him … is within the scope of the Fourth Amendment." 116 U.S. 616, 622 (1886) (emphasis added); *see also id.* at 630 (noting that protections of Fourth Amendment were designed to prevent government intrusions on "the privacies of life"). Like the CTA, the statute at issue in *Boyd* compelled individuals to disclose personal business records to the government for purposes of investigating evasion of customs duties. The Court summarized the history of colonial-era general warrants and writs of assistance and concluded that the statute in question was at odds with a practice the Founders "so deeply abhorred." *Id.* at 630. "It is not the breaking of his doors, and the rummaging of his drawers, that constitute the offense; but it is the invasion of his indefensible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence." *Id.*

The parallels between the statue in *Boyd* and the CTA are plain. But at least in *Boyd* an individual knew the government had targeted him for investigation. By contrast, the CTA not only compels disclosure of sensitive BOI and PII, but it also allows government agents unfettered discretion to probe this information with no reasonable suspicion or notice. The CTA does include statutory protocols and requires FinCEN to draft regulations related to the who, what, when and how a government agency may access the BOI database. But notably absent is any requirement that there be any showing of reasonable suspicion, much

less probable cause, nor is there any opportunity for independent judicial review or notice to an individual targeted by the government. Such broad and imprecise guidelines fall short of the right of individuals to be secure in their persons, property, or papers. "[T]he Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California*, 573 U.S. 373, 398 (2014). Rather, they were concerned about excessive government power to intrude on individual liberty and therefore imposed strict limitations to preserve that hard-fought liberty.

The Appellants asserted before the district court that the Appellees had no expectation of privacy in the BOI required to be produced by the CTA. Dkt. 24-1 at 41-43; Dkt. 40 at 15. Appellants' argument was twofold: (1) neither a subjective nor objective reasonable expectation of privacy attaches to the data required to be produced by the CTA; and (2) the Appellees (and others similarly situated) voluntarily disclosed the BOI to third parties and thus they could not have a reasonable expectation of privacy. Neither assertion is accurate.

Appellants concede that the CTA compels production of BOI and PII that, in many instances, is not required to be produced to a state at the time of incorporation or formation. AOB at 3. In such instances, there has been no voluntary disclosure and the third-party doctrine would not apply. *See United States v. Miller*, 425 U.S. 435, 445 (1976) (holding that bank customer has no privacy interest in account transaction bank records).

But even in instances where there has been some, perhaps limited disclosure, the Appellees still have a reasonable expectation of privacy in the sensitive data. Prior to the passage of the CTA, the Bank Secrecy Act ("BSA") mandated anti-money laundering programs. *See* 31 U.S.C. § 5318(h). In 2016, FinCEN published the Customer Due Diligence ("CDD") Rule, the main thrust of which was to require banks to obtain BOI from customers. 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. § 1010.230. The CDD Rule requires bank account holders to disclose to the institution essentially the same BOI data the CTA now requires individuals to produce *to the government*. But a critical difference is that BOI produced to financial institutions comes with certain Congressionally mandated privacy protections.

Following *Miller*, Congress recognized that bank customers should have a privacy interest in their financial and bank data, and passed The Right to Financial Privacy Act ("RFPA") of 1978. RFPA provides some measure of privacy protection for financial records held by third parties. 12 U.S.C. §§ 3401-3423. Notably, the statute requires law enforcement to follow legal procedures to gain access to the information and requires customer notification when there is a request for financial records, with some exceptions. *See* 12 U.S.C. §§ 3402-3408, & 3413. The DOJ's own Criminal Resource Manual notes that there are only two situations in which a bank is prohibited from notifying a customer of a grand jury subpoena for their records. Crim. Resource Manual § 426. The exceptions

to notification typically involve a specific request from law enforcement where it has established at least reasonable suspicion or some individualized nexus to a specific crime in relation to the bank records requested. Consequently, if Congress sought to put limits on the government's ability to obtain sensitive financial information from third parties—and that now includes BOI that banks obtain pursuant to the CDD Rule—then it stands to reason that a reasonable expectation of privacy attaches to such information.

At the district court, Appellants relied heavily on *California Bankers Ass'n v. Schultz* to argue that plaintiffs had no expectation of privacy. Dkt. 24-1 at 43 (citing 416 U.S. 21 (1973). Appellants' reliance on *Schultz* is misplaced and its applicability to the CTA is questionable. *Schultz* foreshadowed the Court's holding in *Miller*, upholding as reasonable the Bank Secrecy Act's requirement that certain transaction data be reported to the government. *Id.* at 66 (holding that "reporting of domestic financial transactions abridge no Fourth Amendment right of the banks themselves"). It is critical to note, however, that the Court never reached the question of whether the individual bank customers had a privacy interest in the transaction reports, concluding that because they could "not show that their transactions are required to be reported" they lacked standing. *Id.* at 68. Simply stated, *Schultz*, like *Miller*, stands for the uncontroversial proposition that a bank is required to produce to the government transaction data to which that the bank was a party

subject to appropriate legal process. The bank customer's alleged privacy interest was diminished because the bank was a party to the transaction, and it was the bank's records being sought. The critical distinction between the BSA provisions in *Schultz* and the CTA is that the CTA eliminates the bank middleman and disposes of legal process requirements. The CTA demands not bank records, but BOI data directly from the Appellees, which then becomes searchable at will.

It is important to emphasize that the privacy interest Appellees assert is not the compelled disclosure of BOI, but rather the compelled disclosure to FinCEN's database to which state, federal, and foreign law enforcement agencies have unfettered access, with no notice to the plaintiffs. The district court agreed, finding that the injury "is not disclosure itself, but disclosure to FinCEN, the Treasury Department's criminal enforcement division." Dkt. 51 at 11. It is the subsequent unrestricted and unlimited ability to search the data, with no reasonable suspicion or probable cause that transcends reasonableness. "The Fourth Amendment requires that 'those searches deemed necessary should be as limited as possible.' The 'specific evil' that limitation targets 'is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings.'" *United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

The Supreme Court has acknowledged the privacy interests associated with the aggregation of sensitive personal information. In *U.S.*

Dep't of Justice v. Reporters Committee for Freedom of the Press, the Court rejected a Freedom of Information Act ("FOIA") request for an individual's criminal record, or rap sheet, even though the underlying criminal records were publicly available. The Court reasoned that the consolidated rap sheet was an unwarranted invasion of privacy noting that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout a country and a computerized summary located in a single clearinghouse." 489 U.S. 749, 764 (1989); *see also Perry v. CNN, Inc.*, 854 F.3d 1336, 1341 (11th Cir. 2017) ("Supreme Court precedent has recognized in the privacy context that an individual has an interest in preventing disclosure of personal information." (citing *Reporters Comm.*, 489 U.S. at 762)). The CTA and its unrestricted database of sensitive BOI represents an even more egregious invasion of privacy than a FOIA request for a consolidated criminal record.

2. The third-party doctrine is not applicable.

Further, even if some of the BOI has been previously disclosed to a third party, Appellees still retain a reasonable expectation of privacy in the data. In *United States v. Carpenter*, the Court held that there were limits to the third-party doctrine, particularly considering the advent of newer technology. 585 U.S. at 310. "A person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Id.*;

see also United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayer, J., concurring) (noting that one should "not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection").

Carpenter addressed whether the government was required to obtain a warrant to access a cell phone customer's Cell Site Location Information ("CSLI") maintained by cellular phone networks. The Stored Communications Act, at issue in *Carpenter*, allowed the government to compel disclosure of certain telecommunications records if it offered "specific and articulable facts showing that there are reasonable grounds to believe" the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrates issued two such orders and the networks produced stored CSLI for the defendant for the relevant period. The defendant challenged the admissibility of the evidence as a violation of the Fourth Amendment. The Court concluded that the defendant had an expectation of privacy in the CSLI even though he did not possess or control the data. Thus, obtaining the CSLI amounted to a search requiring a warrant issued pursuant to probable cause, far below the standard in § 2703(d) of the SCA. *Carpenter*, 585 U.S. at 316. Returning to the core principles of the Fourth Amendment, the Court concluded that "progress of science has afforded law enforcement a powerful new tool to carry out its responsibilities. At the same time, this tool risks Government encroachment of the sort the

Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Carpenter*, 585 U.S. at 320 (quoting *Di Re*, 332 U.S. at 595).

The expectation of privacy that Appellees have in the BOI is even more compelling than the facts of *Carpenter*. It is the *Appellees* that possess the BOI which the CTA requires production, and not some random third-party. In some instances, Appellees may have produced some of the BOI or PII to a third party for a limited purpose, but that doesn't lessen the Appellees' privacy interest in that data.[2] *See Riley,* 573 U.S. at 392 ("[D]iminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely."). Moreover, the BOI

---

[2] True, the CDD Rule requires a bank or financial institution to obtain the business entity BOI when opening an account. 31 C.F.R § 1010.230. Typically, that information would be disclosed to FinCEN or law enforcement only when the bank's internal compliance function detected something concerning and prepared a Suspicious Activity Report (SAR), or if a law enforcement agency was independently investigating some alleged criminal conduct associated with the account. The investigating agency might then issue a subpoena for the relevant BOI information associated with the account subject only to a relevance standard. Even then, the Fourth Amendment warrant requirement may be implicated, requiring the government to demonstrate probable cause. *See Carpenter*, 585 U.S. at 317 ("[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy."); *see also id.* at 319 (noting that "official curiosity" cannot justify government collection of documents (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 642 (1950)).

and PII required to be produced under the CTA is far more sensitive than location data. Unlike an individual's movements in public that are observable by random members of the public, individuals typically don't publicly disclose sensitive BOI and PII to the general public.

A primary concern driving the Court's decision in *Carpenter* was "the seismic shifts" in technology that dramatically altered the government's surveillance capabilities. *Carpenter*, 585 U.S. at 313. FinCEN's comprehensive government database populated with sensitive personal data that individuals are compelled to produce without any suspicion of wrongdoing similarly represents a powerful new law enforcement tool, particularly with the advent of artificial intelligence. *See, e.g., Jones*, 565 U.S. at 428 (2012) (Alito, J., concurring in the judgement) (noting that unlike the pre-computer era, mass-scale monitoring is now "relatively easy and cheap"). This Court should follow *Carpenter* and "decline to grant the state unrestricted access" to such sensitive data. 585 U.S. at 320.

II. The CTA is ripe for the type of abuse that the Fourth Amendment is designed to prevent.

In *Reporters Committee* the Court acknowledged the privacy interests associated with aggregated sensitive personal information and recognized that there were legitimate privacy concerns with such centralized clearinghouses. 489 U.S. at 764. Those concerns are even more applicable when it is the government that demands production of

the data and then has unfettered access to that aggregated sensitive personal information.[3]

"Fourth Amendment rights are not just a civil liberty, but a substantive check on the power of the state to intrude into and interfere with the privacies of life." Richards, *supra* at 1449. Indiscriminate and "all-encompassing" collection of personal information "poses the danger of government fishing expeditions through database, just as the British had threatened the security of the Founders with the abusive general warrants and writs of assistance that originally inspired the Fourth Amendment." Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 220 (2018) (citing *Carpenter*, 585 U.S. at 311). Justice Sotomayer, joined by Justice Alito, echoed these concerns, stating that the "government's unrestrained power to assemble data that reveal aspects of identity is susceptible to abuse[,]" and is liable to "'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Jones*, 565 U.S. at 416 (Sotomayer, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 295 (7th Cir. 2011) (Flaum, J., concurring)).

---

[3] Even if the collection and aggregation of the data required by the CTA isn't itself a search, the query of the database would be a search and the Fourth Amendment's restrictions are "no less violated because it was accomplished through a [database] query rather than a more traditional search." *See* Emily Berman, *When Database Queries are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 612 (Dec. 2017).

Examples of such government abuse unfortunately have become more frequent. In May 2023, the Foreign Intelligence Surveillance Court unsealed an opinion that detailed abuse by the FBI using Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). 50 U.S.C. § 1881a. The opinion noted that "compliance problems with the FBI's querying of Section 702 information have proven to be persistent and widespread." *[REDACTED] Memorandum Opinion and Order*, Slip Op. at 49 (FISA Ct. Apr. 21, 2022) (released to public May 18, 2023). The level of abuse was extreme: "the FBI illegally accessed a database containing communications … more than 278,000 times, including searching for communications of people arrested at protests of police violence and people who donated to a congressional candidate." Electronic Frontier Foundation, *Newly Public FISC Opinion is The Best Evidence For Why Congress Must End Section 702*, (May 23, 2023); *see also* Jared Gans, *FBI repeatedly misused surveillance tool, unsealed FISA order reveals*, THE HILL (May 19, 2023). And an earlier FISC opinion from October 2018 found that the FBI's querying and minimization procedures under Section 702 fell short of Fourth Amendment requirements. *See [REDACTED] Memorandum Opinion and Order*, Slip Op. at 2-3, 92 (FISA Ct. Oct. 18, 2018).

Databases containing financial data also have been the subject of alleged abuses, allowing the government unfettered access to sensitive financial data. For instance, the Wall Street Journal reported on the

Transaction Record Analysis Center ("TRAC"), a database containing data on more than 150 million money transfers between people in the United States and in more than 20 countries. Dustin Volz & Byron Tau, *Little-Known Surveillance Program Captures Money Transfers Between U.S. and More Than 20 Countries*, WALL. ST. J. (Jan. 18, 2023). According to the report "any authorized law-enforcement agency can query the data without a warrant to examine the transactions of people inside the U.S. for evidence of money laundering and other crimes." *Id.*

More recently, Congress has explored allegations that FinCEN prompted various banks to pursue specific searches regarding customer financial transactions that "keyed on terms and specific transactions that concerned core political and religious expression protected by the Constitution." *Financial Surveillance in the United States: How Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans*, Interim Staff Report, Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government, U.S. House of Rep. (Mar. 6, 2024).

The CTA is tailor-made for similar abuses and infringements upon civil liberties. Indeed, the statute implicitly concedes that such abuses will occur because it incorporates annual audit requirements by Treasury and investigating agencies and both civil and criminal penalties for unauthorized access. *See* 31 U.S.C. § 5336(c)(3)(I-K) & (c)(4).

In *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961), the Court observed that "[t]he Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *See also Jones,* 565 U.S. at 416 (Sotomayer, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms."). As Justice Stewart observed more than 40 years ago, "the mandates of the Fourth Amendment demand heightened, not lowered, respect, as the intrusive regulatory authority of government expands." *Donovan v. Dewey*, 452 U.S. 594, 612 (1980) (Stewart, J., dissenting). The CTA is exactly the type of excessive government intrusion susceptible to abuse that offended the Founders, and it should be rejected as a violation of the Fourth Amendment.

Conclusion

The district court's final judgment granting plaintiffs motion for summary judgement should be affirmed.

Dated: May 20, 2024

Respectfully submitted,

/s/ Neville S. Hedley

Neville S. Hedley
HAMILTON LINCOLN LAW INSTITUTE
1629 K Street NW, Suite 300
Washington, DC 20006
Telephone: (312) 342-6008
Email: ned.hedley@hlli.org

Counsel for Amicus Curiae

Certificate of Compliance

This brief complies with the type-volume limitation of Fed. R. App. Proc. 32(a)(7)(B) because this brief contains 5132 words, excluding the parts of the brief exempted by 11th Cir. R. 32-4, as counted by Microsoft Word.

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

Executed on May 20, 2024 *<u>/s/ Neville S. Hedley</u>*
Neville S. Hedley