

forces brokers, exchanges, clearing agencies, and alternative trading systems (ATS) to capture data on every investor's trades, from inception to completion. The data is then stored in a centralized database that SEC and private regulators can mine for data and analyze in perpetuity. Thousands of people—many of them not even in the government—will have access to this information.¹ No one can opt out of this forced disclosure. Brokers cannot opt out, and neither can Americans executing their own trades, unless they stop trading in U.S. markets. This surveillance database reportedly would be the largest database of securities data ever created,² and the largest database outside the NSA.³ Unlike NSA, however, SEC entirely lacks the authority, history, or special oversight structure that permits it to engage in the seizure and surveillance of private information.

The Panopticon Is Here

At the time of the French Revolution, the British philosopher Jeremy Bentham coined the term “Panopticon” to describe the terror of a prison wherein all inmates would be subject to 24-hour surveillance by an unseen observer.⁴ Such a system was unthinkable for free people, yet today SEC's scheme frighteningly seizes the personally identifiable record of “every order, cancellation, modification and trade execution for all exchange-listed equities and options across all U.S.

¹ *Oversight of the Status of the Consolidated Audit Trail, Hearing Before the S. Comm. on Banking, Hous., and Urb. Affs.*, 116th Cong. (2019) (Testimony of Shelly Bohlin, COO of FINRA CAT LLC), available at <https://perma.cc/G49S-GR3G>

² Secs. Indus. and Fin. Mkts. Ass'n (“SIFMA”), Comment Letter Addressing Notice of Filing Amendment to the Nat'l Mkt. Sys. Plan Governing the Consolidated Audit Trail at 2 (Jun. 30, 2022), available at <https://perma.cc/2Y5Y-AK4H>.

³ *Implementation and Cybersecurity Protocols of the Consolidated Audit Trail: Hearing Before the Subcomm. on Cap. Mkts, Secs, and Inv., H. Comm. On Fin. Servs.*, 115th Cong. 2 (Nov. 30, 2017) (statement of Rep. Bill Huizenga, Chairman, Subcomm. on Cap. Mkts, Securities and Investment), available at <https://www.govinfo.gov/content/pkg/CHRG-115hhrg31288/pdf/CHRG-115hhrg31288.pdf>.

⁴ Jeremy Bentham, *Panopticon; or, the Inspection House* (1791).

markets”⁵ for everyone who trades on an American exchange—at least the Panopticon applied only to persons imprisoned for a crime. Nothing in the securities laws gives the SEC power to regulate investment decisions of Americans nor to gather all investment data from them or their brokers.

Historically, a government that wished to track its citizens had to devote large resources to having them followed. That is no longer the case: modern surveillance tools enable mass tracking of individuals’ every movement, every transaction, every purchase, sale, or transfer of securities at low cost while powerful computer algorithms can process that information to reveal personal and private details of each person’s financial life or investment strategy. With technological surveillance and data-processing technology becoming ever cheaper and increasing exponentially in power—witness the growth in the power of AI and bots over our electronic lives—the only things that stand in the way of this Orwellian “Big Brother” are our laws and our courts. This class-action complaint challenges SEC’s shocking arrogation of power to impose dystopian surveillance, suspicionless seizures, and real or potential searches on millions of American investors.

The Founders’ Vision

The Framers of the Constitution ensured protection of “persons, houses, papers, and effects” from “unreasonable searches and seizures.” U.S. CONST. amend. IV. Knowing all too well how such seizure of papers imperiled their own liberty, the Framers would scarcely believe the unbridled power SEC seeks to exert through the CAT. By seizing innocent Americans’ private financial information and storing it in a giant database that allows broad access by government and non-governmental persons or entities alike, SEC—a mere administrative agency—has conjured

⁵ Press Release, SEC Approves New Rule Requiring Consolidated Audit Trail to Monitor and Analyze Trading Activity (July 11, 2012), available at <https://perma.cc/R9H3-V5QD>.

into being exactly what the Constitution was written to prevent. Equally troubling and unreasonable, this vulnerable warehouse of seized information also exposes data lawlessly extracted from every investing American to easy onslaught from known cybersecurity threats, domestic and foreign, including even the possible theft of their holdings.⁶ These assets comprise the core of Main Street investors' financial security, which is essential to their individual liberty, wealth, well-being, and personal security. The government has no license to put these interests at risk. To the contrary, the Constitution expressly prohibits uncaging this CAT.

“The Fourth Amendment refers to ‘papers’ because the Founders understood the seizure of papers to be an outrageous abuse distinct from general warrants.” Donald A. Dripps, *“Dearest Property”: Digital Evidence and the History of Private “Papers” As Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 52 (2013). Thus, “[i]f one goes back to the early Republic ... it is difficult to find any federal executive body that could bind subjects to appear, testify, or produce records.” Philip Hamburger, *Is Administrative Law Unlawful?* 221 (Univ. of Chi. Press 2014). Indeed, it was so well established at common law that “[p]apers are the owner’s goods and chattels” and “are his dearest property” that “it may be confidently asserted that [these] propositions were in the minds of those who framed the fourth amendment to the constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.” *Boyd v. United States*, 116 U.S. 616, 626-28 (1886) (first and second quotations quoting *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765)). The Supreme Court therefore recognized that “a compulsory production of a man’s private papers” is the same as “[b]reaking into a house and

⁶ Letter from Seven Senators to SEC Chair (July 24, 2019), *available at* <https://perma.cc/3KSA-WEPT>.

opening boxes and drawers,” and constitutes an unlawful “invasion of his inalienable right of personal security, personal liberty and private property[.]” *Id.* at 622, 630.

While the Constitution made clear the government lacks the authority to peek into—much less seize and keep a permanent record of the content of—a person’s private papers without a warrant, SEC has now arrogated the power to demand government seizure of *everyone’s* private trading information without *any* judicial process.

The Stakes Are High

This case requires this court to exercise its Article III duties to declare CAT unconstitutional under the Vesting Clause, art. I, §1; the Taxing and Appropriations Clauses of Article I; and the First, Fourth, and Fifth Amendments. Where Americans and American entities, like Erik Davidson, John Restivo (“Individual Plaintiffs”), and NCPPR, invest in the securities markets, they do not “voluntarily assume[] the risk’ of [the party] turning over” the details of their personal investment activity for review by SEC. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (first alteration in original) (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)). Indeed, Americans expect and have thus far enjoyed the opposite assumption—that the third party *and* the government will respect their contractual and constitutional rights. Defendants have unlawfully violated those rights, liberties, and expectations, in defiance of the Constitution, as set forth below.

Further, the CAT scheme is unlawful because no statute confers authority on SEC to engage in this conduct at all. Indeed, no statute *could* confer such authority—the First, Fourth, and Fifth Amendments forbid it.

Appropriations and Spending by the Executive

The CAT scheme further violates the Constitution and laws of the United States because it bypasses Congress’ power of the purse and erects a multi-billion-dollar scheme in which SEC self-

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.