Public Statement

Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19

Commissioner Hester M. Peirce

May 15, 2020

I write to dissent from the financial incentive amendments to the National Market System plan governing the Consolidated Audit Trail (CAT) that the Commission is adopting today. These amendments use financial penalties to encourage plan participants to get the CAT up and running quickly after years of implementation problems. Rather than encourage the CAT's expeditious completion, we should reconsider the project in light of the clear threat it poses to Americans' liberty and privacy.

Concerned by the 2010 "Flash Crash" and the subsequent difficulty in analyzing the events of that day, the Commission devised a plan in 2012 to create a consolidated audit trail. The Commission could have required self-regulatory organizations (SROs), which include securities exchanges and the Financial Industry Regulatory Authority (FINRA), to develop a tool designed to make it easier for the Commission and SROs to analyze similar market events in the future. Such a tool could have built on existing databases and trade-reporting processes to allow reconstructions of trading patterns preceding significant market disruptions.

What the Commission chose to do in 2012 was very different. It ordered the SROs to create a comprehensive surveillance database that will collect and store every equity and option trade and quote, from every account at every broker, by every investor. This ambitious objective means the CAT must contain, in some form, voluminous amounts of personal and business confidential information. This gigantic database, housing all this information in a single place, will be accessible to thousands of people at the Commission and the SROs, who will be able to watch investors' every move in real time.

As is common with projects of such grandiose scale, CAT implementation has been plagued with repeated delays. Chairman Jay Clayton, having inherited this project, has worked hard to see it through to completion, while also seeking to mitigate the risks it presents. His efforts have borne fruit in the form of changes that should make this information materially less susceptible to misappropriation and misuse by bad actors.[1]

These changes, however, do not address the deeper problem with the CAT, namely the significant costs that a comprehensive surveillance tool of this type presents to Americans' liberty and privacy. The CAT's financial burden has grown increasingly apparent as the implementation process has dragged on. Staff of the SROs, broker-dealers, and Commission have expended countless hours and dollars to build the CAT's intricate regulatory, legal, and technological infrastructure. On the other hand, the costs our rules impose on liberty and privacy often draw less attention, in part because these costs are harder to measure than mere financial costs. However, the CAT's impending launch and the increasing emphasis on the value of the CAT's comprehensive, real-time database as an enforcement tool demand just such an analysis.

As an initial matter, it is doubtful whether the CAT's comprehensive surveillance database will significantly advance the Commission's mission. That mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The Commission's enforcement program is an important tool in pursuing that mission, and the CAT may make it a bit easier to investigate certain types of market misconduct.[2] However, it is unlikely that it will materially change the types or number of enforcement cases the Commission brings. Is this questionable benefit worth the CAT's costs?

Even if the CAT were likely to advance the Commission's mission in a significant way, to determine whether pursuing the CAT further is worthwhile, we need to look carefully at *all* of the costs that the CAT is likely to impose after it is operational. As noted above, some of these costs are economic, but the most important costs are the non-quantifiable costs to society and to the liberty and privacy that all Americans hold dear. Perhaps somewhat counter-intuitively, the Commission needs to take seriously the public's interest in *not* having a single, comprehensive surveillance database that allows thousands of users to track every person's activities in the securities markets.

The non-financial costs of being surveilled reach to the very core of our humanity. Freedom of thought, expression, and action are key to unlocking each person's unique potential to contribute to society. Untargeted government surveillance programs, even well-intentioned ones, threaten that freedom. A fundamental expectation of a free people is to not be subject to unwarranted monitoring.

Our legal tradition recognizes these costs and limits when and how government can gather information about our lives. For example, if the government suspects that someone is planning a murder, it may seek to monitor her communications, but only in compliance with statutory and constitutional safeguards such as the requirement to show probable cause.[3] Getting a warrant or following other required procedures may take time and inconvenience law enforcement officials, but Americans have decided that this burden on government is an acceptable, indeed necessary, safeguard of our liberties. The typical American would find it offensive if law enforcement decided willy-nilly to monitor her communications on the off chance that she might someday decide to plan a murder. Sure, such an approach might allow the police to prevent a few additional crimes each year, but society has decided that the cost would be too high.

Some surveillance defenders might say, "Well, if you are not planning a murder, you have nothing to be worried about." The matter is not so simple; ongoing, unwarranted monitoring imposes costs that fall on the innocent and guilty alike. Being watched can change the way people—even people whose actions are beyond reproach—behave. It eats away at the psyche and soul. It is not only being watched while you act that matters; being watched while you think is also problematic. As Professor Neil Richards has explained, "intellectual surveillance," which he describes as "surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues"—"is especially dangerous."[4] Among other problems, such surveillance dissuades them from exploring ideas that fall outside the mainstream.[5] It also changes the "power dynamic between the watcher and the watched" by exposing the watched to the risk of "discrimination, coercion, and the threat of selective enforcement where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance."[6]

Concerns like these have motivated Americans to resist surveillance that tracks our activities as drivers,[7] bikers,[8] shoppers,[9] readers,[10] and internet searchers.[11] Many Americans find it troubling to have their activities monitored by any organization, public or private. We ought to be particularly troubled when the power of the state requires Americans to acquiesce to such monitoring as a condition of engaging in political, economic, or other activity. If many of us find the notion of a government agent looking over our shoulders while we browse the internet or shop for books obnoxious and a little creepy, should we feel any differently about being watched by the government as we trade?

Some people might say, "Of course it's different: trading history is not protected expression; it is simply information about an economic transaction with no expressive value." However, economic transactions offer a window into a person's deepest thoughts and core values. Our purchases and sales of securities, particularly when aggregated together as the CAT would do, are a rich form of value expression. They might express a view of how markets

work, a determination on the efficiency of markets, expectations about the future, or even a moral philosophy. Investors' trades may flow from a carefully crafted trading strategy based on a person's education, careful data analysis, intuition, or market experience. People may trade to express their belief about how a company, industry, or nation will perform in the short- or long-term. People might sell stock because they fear a recession is coming or buy stock because they anticipate that the election of a particular candidate or party will bring a period of economic prosperity. An investor might buy shares of a movie company because she is sure a particular movie will be popular, shares of a technology company because she believes the company's engineers are geniuses, or the shares of a cellphone provider because she believes a strategic merger is on the horizon.

People's investment decisions—what they buy, what they sell, what they avoid buying—may also or alternatively reflect their moral convictions. An investor may purchase shares of a clothing company because he likes the political messages of its celebrity spokesperson or shares of a restaurant chain because it donates to his favorite charity. On the other hand, an investor may choose to avoid or sell companies that are associated with things he opposes—carbon emissions, dictatorial regimes, alcohol, tobacco, guns, pornography, discrimination, poor treatment of workers, abortion, the military, gambling, shoddy products, or any other of the many things about which people have strong feelings. Another investor may choose to express her defiance of popular sentiment by investing in companies that produce guns, alcohol, or cigarettes. Our markets provide all of these alternatives, and more, to suit the divergent values and tastes of the remarkably diverse investors in our markets.

Investors whose trades are not a direct reflection of granular moral, ethical, or religious beliefs may fear rebukes from other people who view trading decisions as morally motivated. Of course, the Commission and the SROs do not plan to assess investor virtue; rather, they intend to use CAT data to evaluate people's compliance with the securities laws. It should be evident, though, that today's good intentions do not protect against tomorrow's bad actors.[12] One can imagine a future in which a delectably large database of trades becomes a tool for the government to single people out for making trading decisions that reflect—or are interpreted to reflect—opinions deemed unacceptable in the reigning gestalt. This concern may be premature, but thinking about it seriously now is necessary to protect the liberty of future investors in our markets.

Given their expressive value, untargeted surveillance of financial transactions raises the same types of civil liberty concerns as other mass surveillance programs. The Commission is a securities regulator, and it is tempting to think that First Amendment and other concerns about individual liberty are outside our job description; however, our responsibilities include defending the Constitution, and our rules are part of the legal framework that determines how freely Americans can exercise their constitutional rights. We must take care that our surveillance tools are consistent with these rights. Doing so means recognizing that, as with respect to her other activities, a person's trading activity merits watching only when there is a reason to suspect that she is violating the law. Recognizing this means resisting the desire to surveil a person's every move in the securities marketplace simply because she *might* do something wrong. It means understanding that a person's buying and selling of securities is an expression of what she knows and believes. It means acknowledging that markets are powerful precisely because they draw upon the unique, intensely personal knowledge and expertise of the participants in the marketplace.[13] And finally, it means acknowledging that we cannot, in our desire for investigative efficiency, disregard the liberty and privacy interests of ordinary Americans.

For all of these reasons, it is a mistake to view the CAT as nothing more than an innocuous repository of dry economic data. The CAT will be a comprehensive record of decisions made by millions of Americans that communicate their carefully constructed trading strategies, their opinions about the prospects of particular issuers and industries, and, for some, their moral, ethical, or religious beliefs. That some investors undoubtedly are engaged in misconduct in our financial markets cannot justify amassing this information, especially when more targeted techniques, such as electronic blue sheets, exist.[14] We do not set up mass surveillance programs of other types of activity simply because some of it is illegal. There is no principled basis for treating Americans' activity in financial markets any differently from other types of activity that reflect a person's thoughts, preferences, fears, and hopes.

Moreover, gathering all of this sensitive information in a single database to facilitate more convenient surveillance of investors creates other risks for the very investors the CAT is purportedly intended to protect. Because the surveillance function requires a comprehensive database, the CAT will gather data from thousands of reporting entities, including many that have not previously been required to stream all of their customers' transaction data to an outside entity. Because the surveillance function requires eyes to watch and minds to interpret the data, thousands of Commission staff and employees of the participants must have access to the database.[15]

The sheer value and size of the database will make the CAT an inviting target, and the number of users and reporting entities will make it a more vulnerable one. Each of the thousands of users and each of CAT's many contributors will afford a would-be hacker a potential point of entry. Each of these thousands of users will be able to track investors' market moves, and, with a little effort, also will be able to reconstruct and misappropriate proprietary and confidential trading strategies.

My colleagues are taking the security of the CAT very seriously, as are the SROs, but such a large database will remain an attractive target. As noted above, Chairman Clayton has directed—and the rest of the Commission has embraced—numerous, welcome changes to the CAT to make it more secure. In addition, the Commission and the SROs will continue to take considerable steps to screen employees carefully to weed out potential bad actors. After all, the reputation of each of these organizations depends largely on the quality of its employees, and on their prudence, discretion, and responsibility in fulfilling their critically important functions. Even the most vigilant employer, however, cannot identify every possible bad actor, and one security lapse involving only one of the CAT's thousands of users could compromise the entire database. Moreover, even an honest employee can become the inadvertent conduit for a cyber-breach. If history is any guide, unauthorized access to, or disclosure of, the information contained in the CAT is almost certainly just a matter of time.[16]

Given these risks, we should eliminate the CAT. As Justice Roberts said, "Privacy comes at a cost." [17] In this instance, that cost would not be terribly high. The Commission's enforcement program already performs very well without the CAT. If the Commission believes the program needs further improvement, we could enhance both the rules regarding responses to electronic blue sheets and FINRA's Order Audit Trail System (OATS). Both tools already allow us to get the information we need, and incremental improvements to reduce delays and errors could make our investigations more efficient without sacrificing Americans' liberty and privacy.

Because we should be working to shelve this well-intentioned, but ill-conceived project, not encouraging its quick completion, I cannot support the Commission's action today.

---

[1] The CAT originally would have contained PII for each investor, including social security number or individual taxpayer identification number, date of birth, current name, current address, previous name, and previous addresses. Joint Industry Plan; Order Approving the NMS Plan Governing the CAT, Exchange Act Release No. 34-79319, 81 FR 84696, 85032 (Nov. 23, 2016), *available at* https://www.govinfo.gov/content/pkg/FR-2016-11-23/pdf/2016-27919.pdf. The SEC approved an order in March of this year allowing for the generation of an ID number, which would replace individual social security numbers in the main CAT database, and would exempt the reporting of dates of birth and account numbers associated with natural person retail customers to the CAT, and require broker-dealers to report the year of birth instead of full birthdate. *See* Order Granting Conditional Exemptive Relief, Exchange Act Release No. 34-88393, 19-20 (March 17, 2020), *available at* https://www.sec.gov/rules/exorders/2020/34-88393.pdf.

While the exemptive order was an important step in the right direction, investors remain at risk. These measures do not adequately anonymize the data contained within the CAT, and identification of individual investors from the remaining PII may still be possible. Indeed, one study, using 1990 census data, found that 87 percent of the U.S. population "had reported characteristics that likely made them unique" based on three pieces of information taken together: zip code, birth date, and sex. *See* Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP3, 2000), *available at*

https://dataprivacylab.org/projects/identifiability/paper1.pdf. Of course, the CAT database will contain much more than this simple information.

[2] For example, when Commission or SRO staff identify suspicious trading activity, they generally need to use electronic "blue sheets" to request information about the account engaged in that activity from the broker-dealer that submitted the order. Although broker-dealers are required to respond promptly and accurately to these requests, some broker-dealers do not. Because the CAT would allow Commission and SRO staff to link transactions with account-specific information, they may be able to avoid these occasional problems. Reforms short of a CAT could address these problems without the same threat to liberty and privacy.

[3] *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (holding that police's obtaining of cell-site location data that revealed a person's whereabouts over a period of time via court order but without a search warrant violated the Fourth Amendment protection against unwarranted searches); *Katz v. United States*, 389 U.S. 347 (1967) (holding the Fourth Amendment requires that police obtain a search warrant to wiretap a public payphone and stating that "the Fourth Amendment protects people, not places.").

[4] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1935 (2013).

[5] *See id*. ("Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.").

[6] *Id*.

[7] *See, e.g.*, Stephanie Foster, *Should the Use of Automated License Plate Readers Constitute a Search after Carpenter v. United States*, 97 Wash. U. L. Rev. 221 (2019) (discussing the Fourth Amendment implications of automated license plate readers).

[8] *See, e.g.*, Jon Schuppe, *Google tracked his bike ride past a burglarized home. That made him a suspect.*, NBC News (Mar. 7, 2020) (reporting a police request for Google data stored in RunKeeper to help discover potential suspects who were in the area of a crime), *available at* https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

[9] *See, e.g.*, *How and Why Retail Stores Are Spying on You*, Consumer Reports (Mar. 2013) (discussing the many methods stores use to collect data about shoppers), *available at* https://www.consumerreports.org/cro/2013/03/how-stores-spy-on-you/index.htm; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2012) (discussing store's use of analytics to guess with a high degree of certainty that a teenager was pregnant and target her with relevant product advertisements), *available at* https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#783b07fb6668.

[10] *See, e.g.*, Zoe Carpenter, *Librarians Versus the NSA*, The Nation (May 6, 2015) ("Librarians have frequently been involved in the fight against government surveillance."), *available at* https://www.thenation.com/article/archive/librarians-versus-nsa/.

[11] For example, competing privacy and national security interests relating to government surveillance of internet browsing history have generated considerable controversy over the past several years. *See, e.g.,* Robert Goodlatte, *Our digital privacy is at stake in the Senate*, The Hill (May 11, 2020) (discussing proposed amendment to Senate bill that would have required a tougher standard for government investigators to obtain browsing history of individuals), *available at* https://thehill.com/opinion/technology/496578-our-digital-privacy-is-at-stake-in-the-senate; Ellen Nakashima, *FBI wants access to Internet browser history without a warrant in terrorism and spy cases*, Washington Post (June 6, 2016) (describing proposed amendment to Electronic Communications Privacy Act "to give the FBI explicit authority to access a person's Internet browser history and other electronic data without a warrant in terrorism and spy cases" and noting ongoing opposition by civil liberties organizations and technology firms), *available at* https://www.washingtonpost.com/world/national-security/fbi-wants-access-to-internet-browser-history-without-a-warrant-in-terrorism-and-spy-cases/2016/06/06/2d257328-2c0d-11e6-9de3-6e6e7a14000c_story.html. Use of information gathered from users' internet histories by private-sector firms has

also generated considerable controversy. *See, e.g.*, Greg Bensinger, *Never-Googlers: Web users take the ultimate step to guard their data*, Washington Post (July 23, 2019) (detailing consumers' efforts to "wrest greater control of their personal data" from large search and advertising companies), *available at* https://www.washingtonpost.com/technology/2019/07/23/never-googlers-web-users-take-ultimate-step-guard-their-data/.

[12] Dissenting from an opinion that permitted warrantless wiretapping of telephone lines, Justice Brandeis famously observed that "[e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent." *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting). It took the Supreme Court nearly four decades to overturn *Olmstead*. *See Katz v. United States*, 389 U.S. 347 (1967). We need not take so long to reverse our own intrusion on Americans' liberty interests.

[13] *See, e.g.*, Friedrich von Hayek, *The Pretence of Knowledge*, Nobel Prize Lecture (Dec. 11, 1974) (discussing how the sum of the knowledge of individual participants will create a well-functioning market possessing knowledge which no one individual could possess), *available at* https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture/.

[14] *See* note 2, *supra*.

[15] The CAT is required to be able to support a minimum of 3,000 users at one time, but the actual number of users may be higher. *Amended CAT NMS Plan for Consolidated Audit Trail, LLC*, FINRA CAT, 106, n. 61 (Aug. 29, 2019) (stating that although the request for proposals "required support for a minimum of 3,000 users, . . . the actual number of users may be higher based upon regulator and Participant usage of the system"), *available at* https://www.catnmsplan.com/sites/default/files/2020-02/CAT-2.0-Consolidated-Audit-Trail-LLC%20Plan-Executed_%28175745081%29_%281%29.pdf.

[16] Other government-related and private company databases have been attractive targets. *See, e.g.*, Patricia Zengerle & Megan Cassella, *Millions more Americans hit by government personnel data hack*, Reuters (July 9, 2015) (reporting thefts of government personnel records relating to more than 22 million individuals), *available at* https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709; Office of Inspector General, *Semiannual Report to Congress: April 1, 2013 to September 30, 2013*, SEC, 24-25 (2013) (reporting SEC employee's removal of files containing other SEC employees' personally identifiable information), *available at* https://www.sec.gov/about/offices/oig/reports/reppubs/2013/oig_fall2013.pdf; *SEC Brings Charges in EDGAR Hacking Case*, SEC (Jan. 15, 2019), *available at* https://www.sec.gov/news/press-release/2019-1.

[17] *Riley v. California*, 573 U.S. 373, 401 (2014).