SPEECH

Remarks at the Crypto Task Force Roundtable on Financial Surveillance and Privacy

Paul S. Atkins, Chairman (/about/sec-commissioners/paul-s-atkins)

Washington D.C. | Dec. 15, 2025

Good afternoon, ladies and gentlemen, and thank you for joining us. Let me first begin by thanking Commissioner Hester Peirce and the entire Crypto Task Force for organizing today's roundtable. I should also like to thank our distinguished group of panelists who are brave enough to come to Washington to provide their thoughts on financial privacy in the 21st century. Before I provide my own thoughts, I must echo what Richard [Gabbert] just mentioned by noting that the views I express here today are my own and not necessarily those of the SEC as an institution or of the other Commissioners.

Today's roundtable participants will wrestle with a question that, at its core, is profoundly American: whether people can participate in modern finance without surrendering their privacy. This tension raises important questions. On the one hand, the federal government has an obligation to protect Americans from national security interests and threats, including through measures such as the Bank Secrecy Act[1], which Treasury and other agencies use to deter illicit

finance. On the other hand, being free to conduct one's affairs, including financial affairs, free from government and other surveillance is a core American value.

Crypto has been a forcing function, providing a unique opportunity to consider this question in the context of 21st century technology. Since January, this Administration has highlighted the importance of restoring power to individual Americans and entrusting them to manage their own affairs, including when it comes to crypto.[2]

For our part, the SEC must confront its own record in balancing investor protection and privacy. The Commission has established tools like the Consolidated Audit Trail (CAT), swap data repositories, and Form PF, that it asserted were necessary to protect investors, detect fraud, and safeguard our markets. Unfortunately, the federal government's insatiable desire for data has expanded these tools in ways that increasingly put the liberty of American investors at risk — and saddle them with costs that too often provide little benefit because the government does not even use all of the information that is submitted. For example, while the Commission created the CAT with the good intention of providing a clearer view of trading across markets, it became a powerful system that moved the SEC closer toward mass surveillance. That is why we have taken steps to scale back some of the CAT's most sensitive data elements and to re-examine its scope and its cost.

Friedrich von Hayek, in his book, *The Fatal Conceit*, decried the belief of many in government that the solution to problems is to get enough smart people in a room and then collect enough information that these all-knowing people will somehow forge a perfect solution to the problem at hand based on all of that information. Well, we have seen how poorly — maybe never — that has actually worked in practice. So, how right Dr. Hayek was.

With the advent of crypto, it is no great leap to imagine a steady migration toward a future where the government, and a constellation of intermediaries, can peer into almost every dimension of an individual's financial life. While regulators may have a voracious appetite for data, that proclivity is obviously — and fundamentally — incompatible with the kind of free society that has made America great.

Regulators must therefore remain humble and principled as we embrace the opportunities that crypto presents. In the analog era, financial surveillance was

naturally constrained by paper records, physical distance, and manual processes. These delays, while inconvenient for the government, naturally limited how much information the Commission could obtain about any American investor. However, these constraints have dramatically diminished in the digital era, which is why today's conversation about crypto and privacy-enhancing technologies is especially important.

Public blockchains are more transparent than any legacy financial system ever built. Every movement of value is recorded on a ledger that anyone can inspect. Chain analytics firms are already exceptional at assisting law enforcement with linking on-chain activity to off-chain identities. In other words, pushed in the wrong direction, crypto could become the most powerful financial surveillance architecture ever invented.

Indeed, if the instinct of the government is to treat every wallet like a broker, every piece of software as an exchange, every transaction as a reportable event, and every protocol as a convenient surveillance node, then the government will transform this ecosystem into a financial panopticon.

At the same time, this technology allows for privacy-preserving tools that the analog world could not provide, such as zero-knowledge proofs, selective disclosure, and wallet designs that allow users to prove compliance without handing over their entire financial history or personal details to intermediaries or to the government. One can imagine systems where a regulated platform can demonstrate that its users have been screened, without the ability to retain a permanent, person-by-person map of every payment, trade, or donation.

These tools will also help our markets to continue to function smoothly as they move on-chain. Complete financial transparency inherent to public blockchains can disincentivize important financial markets activity.

For example, many institutions depend on the ability to build positions, test strategies, and provide liquidity without instantly telegraphing that activity to competitors and to predatory traders. If every order, hedge, and portfolio adjustment was suddenly visible in real time, we could invite front-running, copycat behavior, and "pile-on" dynamics that make it harder, not easier, for firms to manage risk. Market-making and underwriting become far less attractive if every inventory imbalance or client flow is immediately exposed to the marketplace.

This technology makes it possible to balance the government's interest in deterring threats to our national security and the American public's interest in privacy. But to best strike this balance, we must make certain that Americans can use these tools without immediately falling under suspicion. Shielding the lawful activity of our citizens from bulk surveillance while still ensuring that our government can perform these essential functions is the best way to protect both national security and our basic civil liberties, while also giving room for innovation to flourish.

So, the stakes here are high — and the questions before us carry profound and enduring implications. As we begin this roundtable, I am eager to hear more from our panelists about how we as a Commission can protect Americans' privacy, as well as how crypto's privacy tools can lessen, rather than increase, the need for mass financial surveillance.

Together, I am confident that we can shape a framework that ensures that neither technological nor financial advancements will come at the expense of personal freedoms.

Unfortunately, other obligations are going to prevent me from attending the entire conference, but I am thrilled to have been here to see you all today. Thank you for your time and attendance. I look forward to a robust discussion ahead.

---

[1] We take our delegated authority to enforce the Bank Secrecy Act seriously. When it comes to digital financial technologies, the PWG Report concluded that "American entrepreneurs and software developers should have the liberty, and regulatory certainty, to upgrade all sectors of our economy using these technologies." The PWG Report also recommended that Congress codify the principle that "a software provider that does not main total independent control over value should not be considered as engaged in money transmission for purposes of the BSA." PWG Report, *supra* at 6.

[2] In his very first week back in the White House, President Trump issued an Executive Order on Strengthening American Leadership in Digital Financial

Technology specifically to promote leadership in digital assets and financial technology *while protecting economic liberty*. Exec. Order No. 14178, 90 Fed. Reg. 8647 (Jan 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/; https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/ (https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/)In addition, as directed by the Executive Order, The President's Working Group on Digital Asset Markets issued a report concluding that the working group "supports civil liberties protections surrounding privacy and the ability of individuals to privately transact on public blockchains." The President's Working Group on Digital Asset Markets, *Strengthening American Leadership in Digital Financial Technology* 111 (July 30, 2025), https://whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf (https://whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf) ("PWG Report").

Last Reviewed or Updated: Dec. 15, 2025