

# CBDC Spells Doom



for Financial Privacy

*By Nicholas Anthony*

The government has been undermining Americans' financial privacy for decades. A central bank digital currency would be the final nail in the coffin.

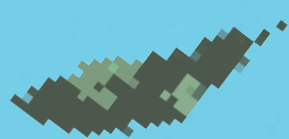




ILLUSTRATION BY THE HEADS OF STATE





Imagine a world where government agencies have instant and complete access to the financial activity of every citizen by default. Regardless of whether you are a business owner or a gig worker, a politician or a dissident, a gun owner or an environmentalist, all of your financial activity would be stored on a central ledger controlled by the government. Left to the whims of political appointees and faceless bureaucrats, an omnipresent surveillance state would loom over every interaction, and financial activity could be frozen in an instant.

This is not the plot of the latest dystopian thriller to hit streaming services. It is the potential future of our financial system under a digital national currency known as a central bank digital currency (CBDC), and that future may not be so far away.

For decades, lawmakers and unelected officials have been chipping away at Americans' financial privacy with laws designed to counter terrorism, catch money launderers, and collect taxes. Yet, just as Americans are beginning to take notice and call for better financial privacy protections, it seems some government officials are looking to create the most sweeping form of financial surveillance seen to date in the form of a CBDC.

Put simply, a CBDC could spell doom for what few protections remain, because it would establish a direct line between each citizen's financial activity and the federal government. And in doing so, a CBDC would further entrench decades of financial surveillance that should be reformed, not expanded, in the digital age.

### **The Dismal State of Financial Privacy Today**

Before we can decode what a CBDC might mean for the future of money, it's

important to establish context. Americans might think payments made with a credit card or payment app are protected from the prying eyes of the government, but financial privacy in the United States is only an illusion.

For many people, this statement might come as a shock. After all, the Fourth Amendment to the Constitution is meant to protect us from sweeping surveillance:

**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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.**

Why shouldn't we feel a sense of protection? It's right there, in our Constitution: "To be secure in one's papers and effects from unreasonable searches and seizures" seems to suggest that financial records should be protected. What are financial records, if not one's papers and effects?

Unfortunately, Congress and the Supreme Court see things differently. In 1970, the Bank Secrecy Act was created to give the government a way to start keeping tabs on Americans' finances. In its earliest form, the Bank Secrecy Act ushered in two major changes. First, it required financial institutions to maintain records on customers "where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." And second, it required financial institutions to report that information to the government in certain circumstances.

Given its drastic deviation from the spirit of the Fourth Amendment, the law was almost immediately challenged in the courts.

Eventually, the issue made it all the way to the Supreme Court, which held that law enforcement does not need a warrant when seeking an individual's financial records at a bank because "the depositor takes the risk, in revealing his [or her] affairs to another, that the information will be conveyed by that person to the Government." In other words, the Court held that records maintained by a third party such as a bank, credit union, or payment app were not protected by the Fourth Amendment. This decision came to be known as the "third-party doctrine," and its ramifications have had an impact on issues far beyond the collection of financial records alone.

Government officials were hardly satisfied with this already substantial deviation from the Constitution. Fast-forward 30 years after the passage of the Bank Secrecy Act, and we face the Patriot Act. Another 20 years later, we see proposals to surveil accounts with as little as \$600. Let's look at each in turn.

The Patriot Act was a response to the terrorist attacks of September 11, 2001. Of course, stopping terrorism is a worthwhile endeavor, but it should not come at the cost of sacrificing the very foundation this country was built upon. Yet, Congress did just that. The Patriot Act dramatically reduced financial privacy by introducing new requirements for banks to identify customers, expanding the reports banks are required to file on those customers, and prohibiting banks from notifying customers when those reports are filed.

Again, government officials were hardly satisfied. Twenty years after the passage of the Patriot Act, the Biden administration pushed for more financial surveillance with

a proposal to monitor every bank account with at least \$600 in annual activity. Outrage ensued as people asked questions like "Doesn't the Fourth Amendment protect us?" and "Why don't we have stronger financial privacy protections?" In a telling moment, the Treasury Department defended the proposal, saying, "In reality, many financial accounts are already reported on to the IRS, including every bank account that earns at least \$10 in interest. And for American workers, much more detailed information reporting exists on wage, salary, and investment income."

While true, the Treasury Department's statement reveals the dismal state of financial privacy in the United States. In 2022 alone, financial institutions filed over 26 million Bank Secrecy Act reports on Americans. Complying with these requirements cost US financial institutions an estimated \$45.9 billion, and the vast majority of the reports were for simply moving more than \$10,000. Yet even that number is an issue. Because the Bank Secrecy Act's reporting thresholds were not enacted with an adjustment for inflation, the net for authorities to cast becomes wider and wider each year with a positive inflation rate (i.e., most years). So, what was set at \$10,000 in the 1970s would be over \$75,000 today.

The problems do not stop there. Law enforcement has also increased its financial surveillance efforts. Between 2019 and 2022, US Immigration and Customs Enforcement (ICE) was collecting batches of records every six months on transfers to or from Mexico greater than \$500. In total, ICE collected around 6 million financial records without so much as a warrant.

Make no mistake, the Treasury Department is right: Financial privacy

is already in a bleak state. Sweeping legislation, legal investigations, and even inflation have all steadily decreased the amount of financial privacy in the United States.

But that doesn't mean things couldn't get worse.

### **A CBDC Spells Doom for What Little Privacy Is Left**

After reading at length about how dismal the current financial system is in terms of protecting Americans from government surveillance, it may be difficult to imagine how things could become much worse. However, things *certainly* could be worse. One of the few benefits of the current system is that there is at least an air gap between the government and the private sector that acts as a buffer between your information and complete surveillance. Introducing a CBDC could very well serve to close that gap and unleash financial surveillance from its few remaining limitations.

Before moving forward, however, some definitions are in order, given many people have been left out of the conversation when it comes to CBDCs. For instance, when surveyed by the Cato Institute in early 2023, 49 percent of Americans said they did not know enough about CBDCs to support or oppose them. Later that year, the Chartered Financial Analyst Institute found similar results in a global survey. So what exactly is a CBDC?

Put simply, a CBDC is a digital national currency that is a direct liability of the central bank. So, in the case of the United States, a CBDC would be a digital form of the dollar. Yet unlike the digital money that countless people already use today via credit cards, debit cards, payment apps,

cryptocurrency, and the like, a CBDC would ultimately be controlled and maintained by the federal government.

Governments around the world are already pushing forward with this idea. According to the Human Rights Foundation's CBDC Tracker, the 11 islands and eight countries that compose the Eastern Caribbean Currency Union have already launched CBDCs; 37 countries, the Eurozone, and Hong Kong have CBDC pilot programs; and 67 countries, two currency unions, and Macao are researching CBDCs. In other words, most governments are currently pushing forward with CBDCs, and some have even launched them. For its part, the United States is currently in the pilot phase.

With that said, how could a CBDC spell doom for financial privacy? Consider the range of third parties that currently exist in the financial system. While these third parties might broadly be referred to as financial institutions, what we are really talking about is a range of individual banks, credit unions, payment apps, and the like. Across the board, these individual institutions serve as both buffers and checks on financial surveillance. If government officials want someone's information, they must find the right financial institution, coordinate with compliance departments, and check the appropriate paperwork. And even then, that institution may not be responsible for maintaining the entirety of someone's financial activity. For example, someone might use Venmo for splitting checks with friends, PayPal to make purchases online, Bank of America for a business account, and Navy Federal Credit Union for a personal account.

To be clear, this system is not ideal and has flaws that must be corrected, but it's

also the last barrier between what little financial privacy exists today and complete financial surveillance.

A CBDC, however, could spell doom for that last remaining buffer of protection because it gives the government a direct line to every person's financial activity. Patrick Schueffel, adjunct professor at the School of Management in Fribourg, Switzerland, described the situation appropriately when he wrote, "Undoubtedly some of these actions can also be taken under the current monetary regime. But CBDCs will facilitate

industry experts Dante Disparte and Marta Belcher have warned, a CBDC would offer a "backdoor directly into your bank account" and "the ability to have absolute visibility into financial transactions." Where the Bank Secrecy Act required banks to report on customers under specific circumstances, a CBDC would allow direct surveillance at all times. Where the third-party doctrine eliminated constitutional protections for information shared with banks, a CBDC would store financial information with the government by default.

**“Put simply, a CBDC could spell doom for what few protections remain, because it would establish a direct line between each citizen’s financial activity and the federal government.”**

matters: going forward these measures can be implemented on a keystroke, in real-time and centrally. No more lengthy data gathering, and alignment of parties will be required.”

In other words, rather than having access only to the more than 26 million reports that financial institutions file in a year and the six million reports that ICE collected, the government would have direct access to everything by default. As cryptocurrency

#### **The Government in Your Wallet**

These concerns might sound extreme, but even the Federal Reserve has confirmed that a CBDC would largely be a tool of surveillance. In 2019, Federal Reserve chair Jerome Powell told Congress, “If it is designed to be financially transparent and provide safeguards against illicit activity, a general purpose CBDC could conceivably require the Federal Reserve to keep a running record of all payment data using the digital currency—a stark difference from cash, for instance—and something that raises issues related to data privacy and information security.” Powell is not alone in making these remarks. European Central Bank president Christine Lagarde said, “When we surveyed Europeans, the first concern that they had in addition to the support to the digital euro was privacy. Privacy is first and foremost on their mind when we develop the digital euro, [but] there would not be complete anonymity as there is with [cash].” And Bank for International Settlements general manager Agustín Carstens said, “We don’t know who’s using a \$100 bill today and we don’t know who’s using a 1,000-peso bill today. The key

difference with the CBDC is the central bank will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability, and also we will have the technology to enforce that.” Plenty of other policymakers have made similar remarks on record, but these three quotes demonstrate that CBDCs pose a very real threat to privacy, and policymakers know it.

Still, some proponents of CBDCs have tried to call for a CBDC design that is mindful of privacy concerns. And to their credit, central banks around the world have slowly started to take privacy concerns more seriously. However, even then, it’s unlikely such efforts will pay off in the long run. From the Bank Secrecy Act to the Patriot Act and the slew of smaller expansions along the way, the government’s track record is clear. One might hope that the data would sit untouched, but history has shown that time and time again, governments have used the financial system as a tool of surveillance and control.

Chris Meserole, former director of the Artificial Intelligence and Emerging Technology Initiative at the Brookings Institution, put it well when asked about his views on CBDCs and the risk of one being used for surveillance in the United States. “I’m not worried about the US immediately going down that road,” he said, “but I do worry pretty significantly that once [a CBDC] is created, all it is going to take is [an awful event such as a terror attack] and suddenly there is going to be immense pressure to use that system in pursuit of different security or criminal justice activity.”

As I explain at length in my book, *Digital Currency or Digital Control? Decoding CBDC and the Future of Money*, which was published by the Cato Institute in June, CBDCs are ill suited for helping financial

inclusion, too late to improve payment speeds, unlikely to advance monetary policy, and unhelpful for maintaining the US dollar’s status as the world reserve currency. With that in mind, there is little reason to justify incurring the risks imposed by a CBDC—even a limited one. When weighing the benefits against the costs, it’s clear that CBDCs are a tool for the government, not the people.

### Looping in Lawmakers

Given what’s at stake, it’s critical that lawmakers and the public understand not only the threats posed by CBDCs but also the need to secure greater financial freedom and privacy in markets today. Luckily, some elected officials are already taking steps to stop CBDCs and strengthen protections for financial privacy.

The Cato Institute’s work has been instrumental in laying the foundation to oppose CBDCs. In 2023, we published an interactive study, “The Risks of CBDCs: Why Central Bank Digital Currencies Shouldn’t Be Adopted,” and a comprehensive policy analysis, “Central Bank Digital Currency: Assessing the Risks and Dispelling the Myths.” The latter marked Cato as the first think tank to craft a legislative framework prohibiting the Federal Reserve and the Treasury from issuing a CBDC in any form.

To make sure this work gets into the right hands, my colleagues and I here at the Cato Institute’s Center for Monetary and Financial Alternatives (CMFA) have made it a priority to spread the word on Capitol Hill about the risks of CBDCs. Many members of Congress have since recognized what is at stake and subsequently introduced legislation. For example, Rep. Tom Emmer (R-MN) introduced the CBDC Anti-Surveillance State Act, and Sen. Mike Lee (R-UT) introduced the No CBDC Act.

Both bills were designed to prohibit the Federal Reserve and the Treasury from issuing a CBDC without explicit authorization from Congress.

Just days after Representative Emmer introduced an updated version of his bill in September 2023, CMEA director and Cato vice president Norbert Michel testified before the House Financial Services Committee to explain why the US government should not create a CBDC. Less than a year later, the House passed Emmer's bill.

On the financial privacy front, Rep. John Rose (R-TN) joined the Cato Institute for an event where he discussed his Bank Privacy Reform Act—a bill that would prevent the government from accessing consumers' transaction history without first obtaining a warrant, thus reaffirming the Fourth Amendment protections against unreasonable searches and seizures. In addition, Rep. Warren Davidson (R-OH) introduced the Financial Crimes Enforcement Network Improvements Act to create greater oversight of financial surveillance, and Senator Lee introduced the Saving Privacy Act to adjust mandatory reporting thresholds for inflation.

Each of these bills reflects policy recommendations offered by my CMEA colleagues and me, highlighting a growing political appetite for protecting Americans' financial freedoms.

### **The Path Forward**

Although much of the public is still in the dark when it comes to risks posed by CBDCs, people are increasingly starting to speak out. In fact, the threat to financial privacy posed by CBDCs has raised alarms as a leading concern across academia, industry, and even the government itself.

William J. Luther, an economics professor at Florida Atlantic University, warned, "At

some point, a CBDC that fails to provide a high degree of financial privacy will be used to monitor and censor the transactions of one's political enemies. It is foolish to think otherwise." Likewise, Deborah Matthews Phillips and Mickey Marshall of the Independent Community Bankers of America pointed out that "the creation of a CBDC will introduce significant privacy and cybersecurity risks into the nation's monetary system and disrupt the stability of America's banking system." And in Congress, Rep. Andy Barr (R-KY) said, "The prospect of government surveillance of Americans' individual financial transactions through a CBDC and Fed accounts raises serious privacy concerns."

Considering that the Bank Secrecy Act was passed in 1970 as a way to monitor foreign accounts and is now responsible for over 26 million reports on Americans a year, it should be no surprise that people are worried about the threat a CBDC could pose to financial privacy. There is little doubt that government officials will tout the risks of terrorists, drug cartels, and money launderers to justify the surveillance that a CBDC would bring. But surveilling "for bad actors" inevitably means surveilling innocent people as well. It's time to reduce financial surveillance, not further entrench it. Introducing a CBDC would mark the end of what little financial privacy is left in the United States. ✦

### **ABOUT THE AUTHOR**

Nicholas Anthony is a policy analyst at the Cato Institute's Center for Monetary and Financial Alternatives and a fellow at the Human Rights Foundation. He is the author of the newly released book *Digital Currency or Digital Control? Decoding CBDC and the Future of Money*.