Forbes

The U.S. Should Disavow CBDCs And Set The Standard For Protecting Financial Privacy

Norbert Michel

March 2, 2022

It took Canadian Prime Minister Justin Trudeau less than one week to reverse his decision to invoke the Emergencies Act. Trudeau had used that authority to quash the Freedom Convoy protestors in Ottawa, freezing the bank accounts of individual protestors, crowdfunding platforms, and their payment service providers, but civil liberties groups maintain that the Emergencies Act should not have been used to quell nonviolent protests.

Perhaps Trudeau did overreach, but Americans should be under no illusion: The very same principles that enabled Trudeau to freeze Canadians' bank accounts are engrained in U.S. law and regulation.

In fact, the United States has spent decades leading most developed nations down the same path, discounting fundamental principles in the name of preventing money laundering, tax evasion, and terrorist financing. Central bank digital currencies (CBDCs) could very well end up the crowning achievement of those efforts, but regulators already have enormous discretion and leverage over banks and other financial institutions.

The most recent display of this kind of power in the United States was Operation Chokepoint, when a group of bureaucrats from several independent federal agencies (including the Federal Deposit Insurance Corporation) started shutting legal businesses out of the banking system. It primarily targeted small dollar lenders, firearms dealers, and several other politically disfavored industries.

Although it may be surprising, federal banking regulators were not guilty of anything illegal in Operation Chokepoint.

In 2003, the FDIC issued guidance stating that "institutions face increased reputation risks when they enter into certain arrangements with payday lenders, including arrangements to originate loans on terms that could not be offered directly, by, the payday lender," and that "payday lending raises many consumer protection issues and attracts a great deal of attention from consumer advocates and other regulatory organizations, increasing the potential for litigation."

If the FDIC – or any federal banking regulator – issues this kind of guidance, there is virtually no recourse for a bank. They must comply because regulators can ultimately revoke their federal deposit insurance and shut them down. If regulators deem, for example, that lending to fossil fuel companies puts a bank's reputation at risk, or that doing so constitutes an unsafe or unsound practice, they can force the bank to change its lending behavior and customer base.

That sort of leverage has many climate change activists excited, but their elation is rather short-sighted. If public opinion shifts, or if different views shape agency policies, the very same authority could then be used to target, for example, renewable energy companies.

Or, worse, regulators could use their authority to target groups engaged in constitutionally protected political protests. Much like the Canadian situation, it would be very easy for federal regulators to argue that a large protest endangers the economy and, therefore, the banking system. Even if the protestors are ultimately able to win a court battle, their victory would come long after the end of the protests.

The only way for the government to remain neutral is to stay out of it, and that's virtually impossible under the current system. It would require a near 180-degree reversal in the regulatory approach undertaken by the United States and most national governments.

More narrowly, it would also require a major reversal in the expansive anti-money laundering and know your customer (AML/KYC) rules. Thanks to those rules (in large part, foisted on the rest of the world by the United States), there is virtually no such thing as financial privacy.

Though most avid supporters of cryptocurrency are still holding out hope that the new technology can help strengthen financial privacy, they no longer deny the reality of the AML/KYC regime. They now know, for example, that any third-party intermediary assisting in a cryptocurrency transfer–third party exchanges and wallet providers, such as Coinbase–must abide by all the same AML/KYC rules required of banks and other financial firms.

Crypto users–as well as anyone who prefers to use paper currency–should also come to grips with how harmful a retail based CBDC would be if it is employed in the existing legal framework. Both the narrowly focused AML/KYC rules, as well as the broader operational regulations, ensure that governments can use CBDCs to secure full control of individuals' money and disintermediate the private financial sector.

This sort of control over people is incompatible with a free society, and the United States should be leading the charge in the opposite direction.

Fortunately, it's not too late to renounce launching a retail-based digital currency, or to make up for past mistakes that infringed on law-abiding citizens' privacy. The United States should never have led the way in criminalizing the use of money, or in designating private companies as law enforcement. It should have done all that was necessary to strengthen the protections guaranteed by the Fourth Amendment to the Constitution, and to foster strength and diversity through competition in private financial markets.

The United States' comparative advantage is supposed to be in protecting individuals' rights against government overreach. It can affirm that position of leadership by setting the standard for personal financial privacy. Financial technology has evolved so much that this leadership is more important than ever.

I am Vice President and Director of the Cato Institute's Center for Monetary and Financial Alternatives.