The Cantillon Institute *Working Paper Series: The Dollar Displacement Thesis Working Paper No. 7 T.H. Thornton* 2025

The Permanent Record: Surveillance, Censorship, and the Architecture of Control in the Stablecoin Payment Layer

Abstract

The surveillance architecture of the stablecoin payment layer is not incidental to the technology. It is constitutive of it. This paper identifies and analyzes the specific surveillance and censorship mechanisms embedded in the stablecoin infrastructure that the GENIUS Act has legally mandated: the permanent, public, immutable blockchain transaction record; the smart contract freeze function operable without judicial process; the mandatory government compliance infrastructure; and the discretionary issuer censorship authority that extends beyond government orders. The central argument is that the legislative prohibition on a U.S. central bank digital currency, justified on grounds of surveillance risk and individual privacy, produced a private payment architecture with greater surveillance capacity than any CBDC proposal it displaced. A government-issued CBDC would have operated under Fourth Amendment jurisprudence and direct legislative constraint. The stablecoin architecture places the surveillance and censorship functions in private hands, removes them from constitutional accountability, mandates compliance with government orders as a condition of issuer licensure, and records every transaction permanently on a publicly accessible ledger. The paper documents the operational scale of these functions: Tether's 7,268 blacklisted addresses and approximately $3.29 billion in frozen assets; Circle's 372 blacklisted addresses and $109 million frozen; the March 2026 DFINITY incident that demonstrated the collateral damage of automated transaction graph analysis; and the extraterritorial extension of U.S. freeze authority through the

GENIUS Act's foreign issuer provisions. The payment architecture the legislation produced offers consumers a conditionally revocable license to transact, administered by private entities with no constitutional accountability and no mandatory due process obligations.

The Inversion at the Center

The legislative framework that prohibited a U.S. central bank digital currency justified that prohibition on grounds of surveillance risk and individual privacy. Executive Order 14178 (January 23, 2025) stated explicitly that CBDCs "threaten the stability of the financial system, individual privacy, and the sovereignty of the United States." The Anti-CBDC Surveillance State Act, passed by the House in July 2025 on the same day as GENIUS, was framed as a bulwark against government monitoring of individual transactions.

The GENIUS Act, passed simultaneously, constructs a transaction architecture with greater surveillance capacity than any CBDC proposal that preceded it. This is not a contested characterization. It is a structural description of how the technology operates and what the law requires.

A central bank digital currency, as designed in every major proposal studied by the Federal Reserve, would have been a direct liability of the government, auditable, subject to legislative constraint, and operating under Fourth Amendment jurisprudence governing government access to financial records. The stablecoin architecture enabled by GENIUS places the surveillance function in private hands, removes it from direct constitutional constraint, mandates compliance with government orders as a condition of operating, and records every transaction permanently on a public ledger accessible to any party with the technical capacity to read it.

The argument that stablecoins protect privacy where CBDCs would not require a precise definition of privacy that excludes permanent public transaction records, private issuer freeze authority, mandatory government compliance infrastructure, and retroactive surveillance capacity. No such definition exists in ordinary usage.

The Technical Architecture of Surveillance

Blockchain transactions are permanent, public, and immutable. Every USDC or USDT transaction is recorded on a public ledger: Ethereum, Tron, Solana, or other supported chains, with a timestamp, sending address, receiving address, and amount. This record cannot be altered, expunged, or sealed. It is not subject to a statute of limitations. It does not require a subpoena to access. It is available in perpetuity to any party, government, law enforcement, private actor, or foreign intelligence service, with the technical capacity to read a blockchain.

This is a fundamentally different surveillance architecture than either cash or traditional bank accounts. Cash leaves no transaction record. Bank accounts generate records held by private institutions, accessible to government through judicial process: subpoena, warrant, or court order, with notice requirements and Fourth Amendment protections in criminal proceedings. Blockchain transactions generate a permanent public record accessible without any legal process whatsoever. The government does not need a warrant to know that wallet address A sent 500 USDC to wallet address B at a specific time. That information is public.

The stablecoin surveillance architecture is therefore not a government surveillance tool in the conventional sense. It is a permanent public record that government, along with every other actor, can read without restriction. The surveillance is total, it is retroactive to the inception of the chain, and it is available to adversaries as well as authorities. The privacy argument deployed against the CBDC, that the government would monitor individual transactions, mislocates the threat. The stablecoin ledger does not give the government more surveillance power than it otherwise has. It gives everyone surveillance power simultaneously, permanently, with no legal process required.

The Freeze Function: Private Censorship with Government Compliance Obligations

The GENIUS Act mandates that all permitted payment stablecoin issuers possess the technical capability to seize, freeze, or burn payment stablecoins in compliance with

lawful orders. This is not a discretionary feature. It is a statutory requirement. Issuers that lack this capability cannot operate legally in the United States.

The freeze function is embedded in the smart contract at the token level. When Circle or Tether blacklists a wallet address, the USDC or USDT in that wallet becomes immediately, completely, and permanently non-transferable. There is no pending state. There is no grace period. There is no appeal process in the code. The affected party's funds exist on the ledger but cannot be moved, spent, or redeemed. The condition persists until the issuer explicitly reverses it, a decision entirely within the issuer's discretion, on no mandated timeline, with no standardized process.

The scale of this authority is operational, not theoretical. Tether has blacklisted more than 7,268 wallet addresses across Ethereum and Tron, freezing approximately $3.29 billion in combined assets. Tether cooperates with more than 275 law enforcement agencies across 59 jurisdictions. The FBI and the U.S. Secret Service have direct integration with Tether's platform, enabling agency personnel to identify and flag wallets for freezing. Circle has blacklisted approximately 372 addresses, freezing roughly $109 million in USDC, operating a more reactive, legally anchored model that generally requires a court order or OFAC designation before acting.

The critical distinction from traditional financial surveillance is the mechanism of action. Bank account freezes require judicial process, a court order served on the bank, with the account holder typically having recourse through legal proceedings. Stablecoin freezes operate at the smart contract level: instantaneous, technically irreversible without issuer action, and in the case of Tether's burn-and-reissue mechanism, capable of permanently destroying the frozen tokens and minting replacement tokens to law enforcement, a finality that no bank account freeze can replicate. Once burned, as one compliance analysis noted, no lawyer, court order, or appeal can restore the destroyed tokens. The funds cease to exist on-chain.

Collateral Damage and the Absence of Due Process

The combination of broad freeze authority, algorithmic transaction graph analysis, and no standardized appeals process produces a predictable failure mode: innocent parties are caught in freezes targeting others, with no clear mechanism for remedy.

In August 2022, Circle blacklisted approximately 81 wallet addresses in response to OFAC's designation of Tornado Cash, blocking roughly 75,000 USDC in funds. Tornado Cash was a privacy protocol used by a range of actors, including many with no illicit intent. Addresses that had used the protocol for legitimate privacy purposes were frozen alongside those using it for money laundering. The OFAC designation made no distinction; Circle's smart contract made no distinction.

In March 2026, Circle executed a mass blacklist action against 16 wallet addresses in response to a sealed civil court order, not a criminal proceeding, not an OFAC sanction, but a civil lawsuit in a New York federal court. One of the 16 addresses froze turned out to be the ckETH Minter Smart Contract operated by the DFINITY Foundation: public, documented bridge infrastructure used by thousands of users with no connection to the underlying civil case. The freeze was the product of automated transaction graph cluster analysis that flagged the bridge contract due to its on-chain connections with the targeted businesses. Circle reversed the bridge contract freeze within days, not because a legal process compelled it, but because the public nature of the error generated sufficient reputational pressure.

What the March 2026 incident established is that smart contract-level freezes are not limited to identified individuals, verified bad actors, or even named parties in legal proceedings. They extend to any address that automated graph analysis associates with a target, including public infrastructure serving thousands of unrelated users, with no advance notice, no judicial finding of connection to the underlying matter, and no immediate remedy for affected parties.

The freeze of a bank account in the United States requires a court order specifying the account holder and the basis for the freeze. The account holder receives notice and has the right to challenge the freeze. The GENIUS Act imposes no equivalent specificity requirement on stablecoin freezes beyond requiring that a lawful order "specifies the payment stablecoins or accounts subject to blocking with reasonable particularity." What

constitutes "reasonable particularity" for a smart contract freeze that propagates through automated graph analysis to public infrastructure has not been litigated. The March 2026 incident suggests the answer is: less than the standard that would apply to a bank account.

Discretionary Censorship Beyond Legal Orders

The GENIUS Act's compliance framework governs freezes pursuant to lawful orders. It does not limit issuers to freezing only pursuant to lawful orders. Both Circle and Tether exercise broader, discretionary freeze authority based on internal risk assessments, ecosystem feedback from blockchain intelligence firms, and their own terms of service.

Research published by Range Security found that in multiple cases, addresses were blacklisted before OFAC issued an official designation; the issuer moved preemptively based on internal intelligence. This means the effective freeze authority extends beyond government-mandated compliance into proactive, issuer-initiated censorship based on proprietary risk models that are not subject to public disclosure, judicial review, or regulatory approval.

The practical consequence for the consumer holding stablecoins as a primary transaction medium is that their ability to transact is subject to two distinct censorship authorities: formal government orders transmitted through the issuer, and the issuer's own risk judgment applied without notice, without process, and without appeal. In neither case does the consumer have the due process protections that apply to bank account seizures. In neither case is the decision-making process transparent, consistent, or subject to external review.

This is not the architecture of a payment system. It is the architecture of a conditionally revocable license to transact, administered by private entities under government compliance obligations and their own discretionary risk models simultaneously.

Extraterritorial Reach and Global Surveillance Export

GENIUS extends this architecture globally through its foreign issuer provisions. Foreign payment stablecoin issuers that wish to access the U.S. market must demonstrate the capability and willingness to comply with U.S. lawful orders, including orders to seize, freeze, burn, or prevent the transfer of stablecoins. Non-compliance results in U.S. market exclusion and civil penalties of up to $1 million per day. The Treasury Department is required to publicly identify non-compliant foreign issuers and prohibit U.S. trading platforms from listing their stablecoins.

The consequence of this structure is that U.S. legal authority, OFAC sanctions, court orders, regulatory directives, extends to stablecoin transactions globally wherever U.S.-market-access-seeking issuers operate. A foreign company holding USDC faces exposure to U.S. freeze authority regardless of where it is incorporated or where its counterparties are located, because Circle's compliance obligations are defined by U.S. law and applied globally across all chains where USDC operates.

This is a significant extraterritorial extension of U.S. financial enforcement authority, achieved not through treaty or bilateral agreement but through the market-access incentive structure of the world's largest economy. Nations that wish to participate in dollar-denominated digital payment flows must accept U.S. freeze and seizure authority as a condition of that participation. This is, as the geopolitical case for stablecoins notes, a form of dollar power projection. It is also the global export of a surveillance and censorship architecture without the procedural protections that govern equivalent domestic enforcement actions.

The Auditable and the Censorable Are the Same Thing

The surveillance architecture argument is frequently rebutted with the observation that blockchain transparency is a feature, not a bug, and that on-chain traceability reduces money laundering, terrorism financing, and sanctions evasion relative to cash. This is partially correct. Blockchain analysis has produced significant law enforcement outcomes: Tether's cooperation with 275 agencies has resulted in fraud recovery, terrorism financing

disruption, and human trafficking investigations. The transactional transparency that enables surveillance also enables accountability.

The error in the rebuttal is treating auditability and censorability as separable. They are not. A transaction ledger that is permanently readable is permanently censorable. A payment medium whose transactions are immutably recorded and whose balances can be frozen at the token contract level by a private entity under government compliance obligations does not offer the consumer a choice between transparency and privacy. It offers a single architecture in which every transaction is visible, every balance is conditionally revocable, and the entity administering both functions is a private company with no constitutional accountability for either.

Tether's CEO has explicitly framed this as a selling point: blockchain-based money is safer than cash because every transaction is traceable. The argument is coherent from a compliance perspective. From a civil liberties perspective, it describes a payment system in which financial privacy, the baseline protection that cash provides and that bank secrecy law extends to account records, has been structurally eliminated, replaced by permanent public records and private freeze authority operating in parallel with government compliance obligations.

The consumer who holds stablecoins as a primary transaction medium has accepted a monetary instrument that records every transaction permanently, can be frozen instantly without judicial process by a private entity, can be burned permanently at law enforcement request, and exposes every counterparty to retroactive surveillance by any party with the technical capacity to read a public ledger. These are not edge cases or theoretical risks. They are the documented, operational characteristics of the instruments as deployed.

The Due Process Gap

The GENIUS Act's "lawful order" definition requires that freeze orders be "subject to judicial or administrative review or appeal as provided by law." This provision applies to the government-initiated freeze pathway. It does not apply to issuer-initiated discretionary freezes. It does not specify the timeline for judicial review. It does not require the issuer to

notify the affected party that a freeze has occurred. It does not create a private right of action for consumers whose funds are frozen on the basis of an overbroad or erroneous order.

In the March 2026 DFINITY incident, Circle reversed the erroneous freeze of the public bridge contract within days, not because a legal process compelled it, but because the public nature of the error generated sufficient reputational pressure. The thousands of users whose transactions were blocked during that period had no legal remedy, no formal process, and no guaranteed timeline for resolution. Their funds were inaccessible not because they were parties to any legal proceeding but because they had used infrastructure that automated analysis associated with parties to a civil lawsuit.

This is the due process gap: a payment system in which errors, overbreadth, and abuse of freeze authority have no mandatory remedy, no consistent timeline, and no private right of action for affected parties. The existing financial system, with all its limitations, provides account holders with notice of freezes, right to challenge in court, and regulatory oversight of the institutions administering the freeze. The stablecoin architecture, as currently legislated, provides none of these protections at the scale and in the form that the dominant transaction medium of the consumer economy requires.

Conclusion

The surveillance architecture embedded in the stablecoin payment layer is not incidental to the technology. It is constitutive of it. The permanent blockchain ledger, the smart contract freeze function, the government compliance mandate, the discretionary issuer censorship authority, and the extraterritorial reach of U.S. lawful orders combine to produce a transaction infrastructure in which every transaction is permanently and publicly recorded; every balance is subject to instantaneous private freeze; every freeze is potentially permanent pending issuer reversal on no mandated timeline; errors affecting innocent parties have no mandatory remedy; issuer-discretionary censorship operates beyond the lawful order framework with no external oversight; and foreign participants in dollar-denominated digital payment flows accept U.S. freeze authority as a condition of participation.

The legislation that constructed this architecture was justified in part by the argument that a public CBDC would enable government surveillance of individual transactions. The argument applies with greater force to the private architecture it produced, with the additional feature that the surveillance and censorship functions are administered by private entities with no constitutional accountability, no mandatory due process obligations, and no public oversight of their discretionary compliance decisions.

The consumer who holds stablecoins as a primary transaction medium has accepted a payment instrument in which the distinction between financial privacy and financial surveillance no longer exists in any operationally meaningful sense. The question the due process gap leaves open is not whether these conditions will produce an abuse of freeze authority. It is whether, when that abuse occurs at scale, there will be any legal mechanism capable of addressing it.

References

Executive Order 14178, Strengthening American Leadership in Digital Financial Technology, 90 Fed. Reg. 8507 (Jan. 23, 2025).

Anti-CBDC Surveillance State Act, H.R. 1919, 119th Cong. (2025).

Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025 (GENIUS Act), S. 1582, 119th Cong., Pub. L. 119-27 (2025).

AMLBot. (2025, December). *Stablecoin freezes 2023–2025: USDC and USDT blacklist activity report*. AMLBot. https://blog.amlbot.com/circle-froze-16-business-hot-wallets-including-a-blockchain-bridge-smart-contract/

Office of Foreign Assets Control. (2022, August 8). *U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/jy0916

Tether Operations Limited. (2025). *TetherFacts: Compliance and enforcement metrics*. Tether. https://tetherfacts.com