COIN CENTER

Tear Down this Walled Garden: American Values and Digital Identity

A blueprint for American leadership in digital identity built on open standards, federated trust, personal privacy, and individual freedom.

Version 4 | September, 2025

Abstract

Financial institutions today are burdened by identity verification frameworks that are simultaneously costly, privacy-invasive, and ineffective at deterring illicit finance. Despite vast surveillance systems built on the foundation of the Bank Secrecy Act (BSA), global authorities estimate that less than 1% of criminal proceeds are ultimately recovered. Meanwhile, individuals are forced to repeatedly surrender their sensitive personal information to centralized databases at tremendous personal risk. Indeed, the very same personal information, when compromised in breaches, can be used to further evade such controls.

This report proposes a path toward an open, decentralized digital identity infrastructure using verifiable credentials, zero-knowledge proofs, and open blockchain ledgers. It calls for the creation of a standard setting initiative amongst already engaged private-sector participants in the cryptocurrency ecosystem, the John Hancock Project. It outlines a five-part federal policymaking strategy: standard-setting, credential certification, permitted acceptance coupled with safe harbors, protection of tool developers, and gradual credential minimization. This approach would create an interoperable, privacy-preserving ecosystem that meets regulatory goals without sacrificing civil liberties.

Authors

Peter Van Valkenburgh
Coin Center
peter@coincenter.org

Ian Miers
University of Maryland
imiers@umd.edu

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open blockchain technologies such as Bitcoin and Ethereum. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies.

Table of Contents

I. Introduction and Executive Summary

It's time for a fundamental rethink of digital identity in the United States. Today's identity verification practices, particularly as implemented under our anti-money laundering (AML) and know-your-customer (KYC) regime, are not only invasive and burdensome—they are also ineffective at achieving their stated goals. These KYC tools, representing the primary instruments at our disposal, demand immense manual effort from dedicated professionals, yet they consistently fail to deliver effective results. The status quo imposes enormous compliance costs, subjects individuals to constant surveillance, and exposes sensitive personal data to breach or abuse. Meanwhile, bad actors slip easily through the cracks. Experts, including the United Nations (UN) and Financial Action Task Force (FATF) estimate that much less than one per cent of global illicit finance is ever intercepted.[1] In short, the system imposes enormous costs and privacy burdens for negligible benefit in stopping crime.

But it doesn't have to be this way. Technological tools now exist that can verify meaningful facts about individuals—such as whether they are on a government sanctions list, whether they are at high risk of fraud, or whether they are old enough to enter into a legal agreement—without exposing their name, address, or other personal information. Thanks to recent advances in verifiable digital credentials (VDCs),[2] zero-knowledge proofs and multi-party compute (ZKPs and MPCs),[3] and open blockchain networks (public, tamper-evident, distributed ledgers),[4] we have all the tools necessary to build a digital identity standard that embodies and protects American values of personal privacy and individual liberty while meaningfully improving the efficiency of efforts to combat illicit finance and national security threats. This report outlines a path built around three paradigm shifts—passportable ID, attribute verification, and dynamic risk assessment—and seven core principles for a privacy-preserving identity system: no backdoor, no phone home, no chokepoint, no honeypot,

---

[1] *See* United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes (2011), available at https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf. (estimating 0.2%), see also Financial Action Task Force, Asset Recovery, FATF-GAFI (2022), https://www.fatf-gafi.org/en/topics/asset-recovery.html.

[2] World Wide Web Consortium (W3C), *Verifiable Credentials Data Model v2.0*, W3C Working Draft (Mar. 7, 2023), https://www.w3.org/TR/vc-data-model-2.0/ ("A verifiable credential is a specific way to express a set of claims made by an issuer, such as a driver's license or an education certificate.")

[3] ZKPs—along with other privacy-sensitive computational innovations like fully homomorphic encryption, and secure multi-party computation—enable users to prove or compute things collaboratively without revealing the underlying data—making trust possible without full transparency. *See generally,* Ryan Lavin et al., A Survey on the Applications of Zero-Knowledge Proofs, arXiv preprint arXiv:2408.00243v1 [cs.CR] (Aug. 1, 2024), https://arxiv.org/abs/2408.00243.

[4] Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet*, Coin Center (Oct. 2019), https://www.coincenter.org/open-matters/.

no leaks, no dead zones, and no lockout. The private sector is ready to build, and even federal regulators like FinCEN have begun to strongly encourage the use of innovative digital identity technologies to improve compliance outcomes while reducing systemic burdens.[5]

The challenge is no longer technological. It is institutional and collective. Identity is a classic public good: valuable to all, but underprovided by the market alone. Everyone wants to use the system that everyone else uses, and so without a trusted focal point—a standard to build around, a seed network to trust—we get nothing but fragmentation. That is where government has a vital role to play.

This report proposes a five-part policy framework to overcome the collective action failure at the heart of digital identity:

1. **Standards**: Encourage open, interoperable standards for maximally privacy preserving identity credentials, revocation, and proofs;
2. **Certification**: Allow credential issuers to be certified by private sector organizations as compliant with those technical standards and have their background or due diligence practices certified by regulators as sufficient for various regulatory goals, e.g. KYC at financial institutions;
3. **Mandates and Safe Harbors**: Require financial institutions to accept certified credentials, and insulate them from liability for good-faith reliance;
4. **Developer Protection**: Clarify that developing and maintaining software tools for user-held identity credentials is not unlicensed money transmission, money laundering, or other criminal conduct whose definitions are prone to overbroad prosecution;
5. **Credential Minimization**: Encourage compliance frameworks to evolve toward data-minimized identity or attribute proofs over time.

These reforms can begin immediately under existing agency authority, using regulatory sandboxes and pilot programs. But Congress must ultimately pass legislation to ensure uniformity, clarity, durability, and protections for user privacy and autonomy. The Blockchain Regulatory Certainty Act and Clinton-era frameworks for open digital infrastructure offer useful templates. Together we can make America, once again, a city upon a hill, not only in the physical world, but across the vast and roiling sea online.

[5] Financial Crimes Enforcement Network et al., *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), https://www.fincen.gov/news/news-releases/joint-statement-innovative-efforts-combat-money-laundering-and-terrorist.

II. The Problem: Privacy Failures and Ineffectiveness of the Current AML/KYC Regime

For decades, the U.S. government has required financial institutions to collect and store identifying information about their customers. These requirements, rooted in the Bank Secrecy Act of 1970 and expanded by the USA PATRIOT Act, are meant to prevent money laundering, terrorist financing, fraud, and other forms of financial crime. But while the logic of "know your customer" may seem straightforward, its implementation has proven deeply flawed—both in principle and in practice.

A. A System That Doesn't Work

Let's start with effectiveness. For all the surveillance and paperwork it demands, the existing AML/KYC regime does remarkably little to prevent illicit finance. The United Nations estimates that only 0.2% of criminal funds flowing through the financial system are successfully seized or frozen under current AML practices.[6] Academic research corroborates this: economist Ronald Pol finds the interception rate to be even lower, 0.1%, and suggests that—as a metric for the efficacy of AML policies—interception rates overstate the case, because most interception happens thanks to other AML-unrelated policing practices like drug busts.[7] In a review of AML enforcement in the UK, Australia, and Canada—each with regimes similar to the U.S.—these policies were found to have a "near-zero impact on crime."[8]

This inefficiency is not due to underinvestment. The financial industry spends upwards of $300 billion globally each year on compliance, with U.S. firms representing a major share.[9] A 2020

---

[6] *See* United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes (2011), available at https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf. (estimating 0.2%), see also Financial Action Task Force, Asset Recovery, FATF-GAFI (2022), https://www.fatf-gafi.org/en/topics/asset-recovery.html.

[7] Ronald F. Pol (2020) Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice, 3:1, 73-94, DOI: 10.1080/25741292.2020.1725366

[8] Ronald F. Pol, *Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?*, 21 J. Money Laundering Control 215, 228 (2018).

[9] Ronald F. Pol (2020) Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice, 3:1, 73-94, DOI: 10.1080/25741292.2020.1725366 ("LexisNexis also examined compliance costs elsewhere. The estimated annual cost was $83.5 billion in five European countries,3 $25.3 billion in the United States, and $2.05 billion in South Africa, or $110.85 billion in the surveyed countries. According to World Bank data, those countries represent 36.5 percent of world GDP (2017). Again, simple extrapolation suggests global compliance costs in the order of $304 billion, or 0.38 percent GDP. [Some estimates are higher still.

LexisNexis study estimated U.S. compliance costs at more than $26 billion annually, with large institutions spending upwards of $10 billion individually.[10] Much of this cost arises from redundant onboarding procedures, sanctions screening false positives, and human-intensive investigations triggered by suspicious activity reports (SARs) that often lead nowhere.[11]

Despite the cost and effort, major leaks—like the *FinCEN Files*—have revealed that suspicious transactions often go uninvestigated for years, even when flagged.[12] Meanwhile, criminals exploit the system's gaps, while ordinary users bear the burden of documentation, delays, and exclusion. Recent advances in AI will only exacerbate these failures and magnify the costs of addressing them with traditional compliance methods. As Bloomberg recently reported:

> A suspected North Korean state-sponsored hacking group used ChatGPT to create a deepfake of a military ID document… crafting a fake draft of a South Korean military identification card in order to create a realistic-looking image… The findings are the latest example of operatives deploying AI as part of their intelligence-gathering work… North Korean hackers used the Claude Code tool to get hired and work remotely for US Fortune 500 tech companies, building up elaborate fake identities, passing coding assessments and delivering actual technical work once hired… ChatGPT initially returned a refusal when asked to create an ID, but altering the prompt allowed them to bypass the restriction.[13]

Proponents of far-reaching AML and KYC controls may reply that low interception figures are beside the point: real success lies in deterrence—criminal transfers never attempted because an identity check stands in the way. That is a reasonable objection to our critique, but the available evidence suggests current methods may be deterring the wrong population.

The World Bank has warned that the "inappropriate implementation" of AML/CFT standards, particularly in emerging markets, "plays a role in excluding millions of low-income people from

---

Thomson Reuters says that companies on average spend 3.1 percent of turnover combating financial crime, or $1.28 trillion globally].").

[10] LexisNexis Risk Sols., *True Cost of Financial Crime Compliance: U.S. and Canada Edition*, at 3–4 (2020), https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-usca.

[11] *Id.*

[12] Int'l Consortium of Investigative Journalists, *FinCEN Files: Dirty Money, Powerful Players, Global Scandal* (2020), https://www.icij.org/investigations/fincen-files/.

[13] Sohee Kim, "North Korean Hackers Used ChatGPT to Help Forge Deepfake ID, Researchers Say," *Bloomberg* (Sept. 14, 2025, 8:00 PM UTC), https://www.bloomberg.com/news/articles/2025-09-14/north-korean-hackers-used-chatgpt-to-help-forge-deepfake-id.

formal financial services."[14] More recent FATF stock-takes concede that their own standards have contributed to de-risking and financial exclusion, especially where institutions face high onboarding costs.[15] Ordinary customers with limited time and resources abandon or postpone account opening; sophisticated criminals, by contrast, adapt. Detailed academic reviews find that organized crime groups simply seek more complex channels, leaving overall detection rates stubbornly low even as compliance spending soars.[16] The technologies advanced in this report aim to reverse that dynamic—minimizing the busy-work that blocks lawful users while deploying proofs that are difficult for even well-resourced adversaries to fabricate.

B. A System That Compromises Privacy and Freedom

If the AML/KYC regime fails to catch criminals, it more than succeeds in compromising the privacy of law-abiding individuals. Every time a person opens a bank account, sends a wire transfer, or signs up for a trading app, they are required to hand over a trove of personal data: name, date of birth, address, Social Security number, photo ID, sometimes even biometric data. This information is not just collected—it is stored, often indefinitely, across dozens of databases operated by both public and private entities.

This centralized and duplicative data collection increases the attack surface for identity theft and fraud. According to the Federal Trade Commission (FTC), identity theft reports reached over 1.1 million in 2022 alone.[17] In many cases, the data used to commit these crimes comes not from user mistakes, but from breaches at financial institutions or data brokers. The 2017 Equifax breach alone exposed sensitive data on more than 147 million Americans.[18]

Beyond data breaches and identity theft, centralized financial surveillance systems carry an even more profound risk: the potential for state abuse. AML/KYC records can be weaponized to control or punish marginalized populations. In Xinjiang, China, authorities used financial transaction data to identify Uyghur Muslims who had stopped buying alcohol or

---

[14] World Bank, AML/CFT: Strengthening Financial Inclusion and Integrity (Focus Note No. 56, April 2008), https://documents.worldbank.org/curated/en/226501468174869061/pdf/566220BRI0Box353729B01PUBLIC10FN56.pdf.

[15] Financial Action Task Force, High-Level Synopsis of the Stock-take of Unintended Consequences of the FATF Standards 4 (2021). https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Unintended-Consequences.pdf

[16] Ronald F. Pol, *Anti-Money Laundering: The World's Least Effective Policy Experiment? J. Pol'y Design & Practice* 3:2, 191–206 (2020); Michael Levi & Peter Reuter, *Money Laundering*, 34 *Crime & Justice* 289 (2006).

[17] Fed. Trade Comm'n, Consumer Sentinel Network Data Book 2022, at 6 (Feb. 2023), https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022.

[18] Fed. Trade Comm'n, *Equifax Data Breach Settlement* (2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

cigarettes—behavior interpreted as a sign of religious devotion and grounds for detention in so-called reeducation camps.[19] In Canada, financial institutions were directed to freeze the personal and business accounts of peaceful protestors involved in the 2022 trucker convoy demonstrations against COVID-19 lockdowns, without judicial process.[20] In parts of the Middle East, women's financial activity is tightly monitored and sometimes restricted by male guardianship systems; for instance, access to banking services may be contingent on male approval, reinforcing gender-based control through economic dependency.[21] These examples illustrate the core danger of over-centralized financial identity systems: they may not always be abused, but when they are, they become a permanent infrastructure of repression and control.

And the US is not immune. Law enforcement agencies increasingly rely on financial surveillance as a substitute for traditional warrants or subpoenas. Programs like FinCEN's Section 314(a) information-sharing network give federal agencies access to customer information from financial institutions with minimal judicial oversight.[22] Financial records, unlike communications, are not currently protected by the Fourth Amendment under Supreme Court doctrine.[23] As the House Committee on the Judiciary noted in a recent staff report:

> Federal law enforcement increasingly works hand-in-glove with financial institutions, obtaining virtually unchecked access to private financial data and testing out new methods and new technology to continue the financial surveillance of American citizens.[24]

---

[19] Geoffrey Cain, The Perfect Police State: An Undercover Odyssey into China's Terrifying Surveillance Dystopia of the Future 135–38 (PublicAffairs 2021); see also Human Rights Watch, "Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims (Sept. 9, 2018), https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

[20] Amanda Coletta, "Trudeau defends using emergency powers against trucker protests," Wash. Post (Nov. 25, 2022), https://www.washingtonpost.com/world/2022/11/25/canada-trucker-protest-emergencies-act/.

[21] Human Rights Watch, "Boxed In": Women and Saudi Arabia's Male Guardianship System (July 16, 2016), https://www.hrw.org/report/2016/07/16/boxed/women-and-saudi-arabias-male-guardianship-system.

[22] 31 U.S.C. § 5318A(b); FinCEN, *Section 314(a) Fact Sheet*, https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

[23] *United States v. Miller*, 425 U.S. 435, 440–43 (1976) (holding bank records are not protected by the Fourth Amendment).

[24] U.S. House of Representatives, *Financial Surveillance In The United States: How The Federal Government Weaponized The Bank Secrecy Act To Spy On Americans.* Interim Staff Report of the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government. December 6, 2024, *available at* https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2024-12/2024-12-05-Financial-Surveillance-in-the-United-States.pdf

That unfettered access generates significant cybersecurity risk, and—more fundamentally— it undermines our democratic system. Data collected from these processes inevitably enables politicized debanking and censorship. That we have so far escaped deeper forms of authoritarian oppression here at home—if indeed we have—begins to look more and more like luck rather than law and constitution. In summary, the tools meant to keep us safe have become an infrastructure of ambient surveillance—one that rarely catches bad actors but routinely puts everyone else at risk.

III. How Should AML/KYC Change? How Should Identification Change?

It doesn't have to be like this. New technologies like verifiable digital credentials, zero-knowledge proofs, secure multi-party computation, and open blockchain networks (all described in the next section) offer new possibilities. Leveraging these tools, the goal of a modernized AML/KYC regime should not be to collect ever larger troves of personal data, but to create a system that is more effective against illicit finance while protecting privacy and freedom. To get there, we must reconceptualize what AML/KYC "compliance" could mean using these technologies. Three paradigm shifts can guide the way and frame the discussion before we dive into the technical specifics:

1. **From Siloed Documentation → Passportable ID**
   Today, every bank, broker, or exchange repeats the same documentation process—collecting photocopies of IDs, storing addresses and social security numbers in their own silo, and recreating the same honeypots of sensitive data. The result is inefficiency, massive compliance costs, and endless data breaches. The alternative is portable, user-held credentials: a "passportable ID" that can be issued once, carried by the individual, and accepted everywhere, reducing duplication and attack surface while improving trust.

2. **From Identity Verification → Attribute Verification**
   The current model asks: *Who are you?* But what regulators usually need to know is far narrower: *Are you over 18? Are you a U.S. person? Are you on a sanctions list? Have you paid rent on a US property for the last 10 years?* By shifting from full identity verification to attribute verification, compliance becomes leaner and less invasive. Financial institutions learn only what they are legally entitled to know, not a customer's full life story. This reduces privacy risk while giving regulators sharper, more targeted assurances. A transition to a system that relies on attributes instead of an entire identity document also expands the set of possible identity sources, potentially increasing access.

3. **From Static Risk Scoring → Dynamic Risk Assessment**
   Traditional AML programs rely on static risk scoring baked into onboarding—an initial judgment that rarely evolves. Criminals adapt, while institutions are stuck with stale files. A better approach uses dynamic, updatable proofs: reputational signals and risk assessments that can evolve over time without exposing raw personal data. This makes compliance both more accurate and more resilient, while preventing institutions from hoarding dossiers of sensitive information.

Some of this AML evolution is already underway. The transparency of early blockchains and the mountains of pseudonymous transaction data available therein have already made it easier and more intuitive to shift some compliance efforts from siloed documentation to shared information available on-chain, from a focus on identities to attributes, and from static to dynamic risk-based scoring. In the paraphrased words of one former Treasury official, *It's much less important that we know that this transaction is from a man named Rami and much more important that we know that it's of a series of recent transactions related to Hamas.*

This trend is both encouraging and worrisome. Encouraging because it means that new technologies are already providing opportunities to rethink our otherwise broken AML/KYC regime. Encouraging because it shows that, at least in the realm of digital assets, new approaches are organically emerging and ready for implementation. Worrisome, because without deliberate efforts to make these new approaches protective of privacy and autonomy, technology could worsen many of the civil liberties issues we face today. A fully public blockchain where everyone's every move is cataloged and stored unencrypted for all time is an even better tool for a tyrannical regime bent on profiling and abusing its citizens than our current banking system.

Therefore, the big question is how can we accommodate these AML shifts—from siloed to portable, from identities to attributes, and from static to dynamic—while simultaneously protecting and strengthening American values like privacy and liberty. That question has an answer that comes in two parts: First, we need to know what principles and interests need protecting, and second, we need to know which technologies can help us guarantee those protections? For the remainder of this section we'll briefly lay out seven core principles of a maximally private digital identity system. In the next section, we'll talk about the technologies that can get us there.

These seven principles should guide any effort to develop a maximally-privacy preserving, censorship resistant identity protocol that enshrines American values of individual privacy, liberty, autonomy, and dignity.

1. **User-Control:** Participation must always be voluntary. A person's autonomy to carry, present, or aggregate identity credentials should be guaranteed by cryptographic design—not merely by policy promises or institutional goodwill.
   No back door.

2. **Surveillance Resistance:** Neither credential issuers, verifiers, nor other third parties should be able to reconstruct or observe an individual's credential transaction graph (the full history of their usage of an identity credential). Privacy should be structurally embedded, preventing passive or active surveillance.
   No phone home.

3. **Censorship Resistance:** Credential holders must be free to use their credentials at will. Apart from legitimate revocation by the issuer, no party should be able to block or prevent a credential from being shared or a proof of some attribute in that credential being provided.
   No chokepoint.

4. **Breach Resistance:** The system should avoid single points of failure. No server—whether controlled by an issuer, verifier, or even the user—should represent a vulnerability for mass credential theft, censorship, or tracking.
   No honeypot.

5. **Network-Level Privacy:** Communications surrounding credential issuance and presentation must protect against metadata leakage, including network-level observers.
   No leaks.

6. **Offline Capability:** Credentials should remain provable and verifiable even without continuous internet access, ensuring resilience in adverse conditions.
   No dead zones.

7. **Resilient Recovery:** Standards should specify secure, transparent self-recovery and multi-party recovery methods to guard against device loss, credential lockout, or key compromise.
   No lockout.

We'll discuss the principles throughout the remainder of this report. For now the reader should remember these seven nos: No backdoor, no phone home, no chokepoint, no honeypot, no leaks, no deadzones, and no lockout. This list of restrictive commandments might make one wonder if a digital identity system could work at all, let alone improve the efficacy of AML and anti-crime efforts. As we'll see, thanks to new technologies pioneered in the cryptocurrency ecosystem, you can have it all: privacy, autonomy, and also compliance and crime deterrence.

IV. Key Technologies Enabling Privacy-Preserving Digital Identity

Imagine if identity worked like your wallet, not like a call center. Right now, proving who you are in a digital context means calling back to some original issuer—logging into a government site, waiting on a bank to verify you, uploading the same driver's license for the hundredth time. It's clunky, insecure, and worst of all, out of your hands. Digital Identity should work like a physical license or membership card; you hold digital credentials issued by trusted parties and present them when needed, without oversharing or losing control of your information. Without a global database cataloging your every move, a walled garden that becomes a prison yard.

Three emerging technologies make a better model possible. First, Verifiable Digital Credentials (VDCs) allow institutions to issue signed claims about you—such as your age, residency, or verified account status—which you carry and control directly. Second, zero-knowledge proofs (ZKPs) and secure multi-party computation (MPC) allow you to prove facts derived from your VDCs—such as that you are over 18, not on a sanctions list, or below a certain risk threshold—without revealing the underlying data in the credential. Third, open blockchains provide a neutral and transparent coordination layer that enables the aggregation of multiple credentials—supporting complex, evolving identity use cases like multi-factor verification and reputation scores—without introducing centralized intermediaries or undermining user control.

Together, these components can form a decentralized, privacy-respecting identity system. You hold your credentials. You selectively prove what's needed. And you rely on public infrastructure—not a vulnerable corporate or government database—to verify that your proofs are valid and your rights respected.

A. Verifiable Digital Credentials: Digital ID You Carry Yourself

Verifiable Digital Credentials (VDCs) are the foundation of a user-controlled identity system. A VDC is a cryptographically signed digital document that proves something about you—such as your age, citizenship, or verified account status—and these can be implemented with advanced privacy features, so that a verifier can check the credential's provenance without calling back to the original issuer. Just as you might carry a driver's license in your wallet, you would hold VDCs issued by banks, government agencies, employers, or other trusted entities in a secure digital wallet that you and you alone control. As we've discussed, digital identity should work like a more privacy-preserving physical license that you hold and show, not like a query to a central database. VDCs are the essential first step in making digital identity work like physical credentials. And with VDCs we can accomplish that first important shift in AML/KYC policy, moving from siloed documentation to passportable IDs.

The structure and terminology of verifiable digital credentials has already been defined by standards bodies such as the World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), and International Organization for Standardization (ISO), and OpenID Foundation (OIDF) international organizations that set open technical standards for the internet—everything from HTML to encryption protocols.[25] Through these technical standards, there is a common outline on how verifiable digital credentials are issued, held, and verified in a way that works across platforms and systems.[26] Under this model, three roles typically interact: an **issuer** (such as a bank or government agency), a **holder** (the individual who receives and stores the credential), and a **verifier** (the party that checks a proof derived from the credential). The model is deliberately flexible, allowing credentials to represent a wide range of claims and to support cryptographic features—like digital signatures and selective disclosure—that ensure authenticity and privacy even in adversarial environments. Under the model, each VDC is signed using an issuer's private cryptographic key, and verifiers use the corresponding public key to check the credential's integrity and authenticity.

Notably, this work has already been evaluated by NIST[27] and further developed under the National Cybersecurity Center of Excellence (NCCoE) as a published reference architecture[28] that can solve financial industry use cases such as onboarding new bank accounts. In the most recent release of the NIST SP 800-63-4 framework for identity proofing, VDCs can be used as digital evidence to achieve Identity Assurance Level 2 (IAL2), which is used by many financial institutions and the healthcare industry for high stakes remote use cases.

Importantly, the verifiable digital credential ecosystem is *federated* by design. No single issuer controls identity. Instead, many independent institutions can issue different attestations about the same person: a bank might attest to your account history, a university to your degree, and a government agency to your citizenship or age. You, as the holder, can collect these credentials from multiple sources and aggregate them in your digital wallet. When needed, you can present proofs drawn from one or several of your credentials to satisfy a verifier's requirements —building a composite, trustworthy identity without surrendering control over your full corpus of identity data to some maintainer of a walled garden, e.g. a Google, Apple, or Office of Personnel Management. Thus, without sacrificing several of our relevant principles— in this

[25] See e.g., World Wide Web Consortium (W3C), *About W3C*, https://www.w3.org/Consortium/ (last visited Apr. 25, 2025).
[26] World Wide Web Consortium (W3C), *Verifiable Credentials Data Model v2.0*, W3C Working Draft (Mar. 7, 2023), https://www.w3.org/TR/vc-data-model-2.0/.
[27] Digital Identities: Getting to Know the Verifiable Digital Credential Ecosystem, https://www.nist.gov/blogs/cybersecurity-insights/digital-identities-getting-know-verifiable-digital-credential-ecosystem (last visited Aug 12, 2025).
[28] Digital Identities - Mobile Driver's License (mDL), https://pages.nist.gov/nccoe-mdl-project-static-website/index.html (last visited Aug 12, 2025).

case user-control, censorship resistance, and breach resistance—VDCs can help accomplish our first and second shifts in AML/KYC policy—moving from silos to portable credentials and from identities to attributes.

A verifiable digital credential with a plain digital signature, however, is in essence just digitized paperwork. Anyone receiving such a credential gets all the same information they would have seen in an analog setting, just digitally verifiable. Worse yet, naive use of antiquated cryptographic approaches can create privacy issues wherein verifiers or even third parties could track and record every time and place a user has used the same credential.[29] Improperly implemented, a naive VDC implementation would violate our principles of surveillance resistance, and network-level privacy.

Looking ahead, we will see that these problems can be rectified via two types of cryptography, now in industrial usage on blockchains, zero-knowledge proofs (ZKPs) and secure multiparty computation (MPC). Using these tools, one could show that they have a valid credential, that it says they are legally an adult, and that they are a U.S. national, without revealing anything else to the verifier. We can even go further; since proofs can verify computation, one could show that their name is not on a sanctions list or that they have a certain reputation, without revealing any other information.

However, this turns out not to be enough. First, credentials—whether a plastic driver's license or a digital version now available on smartphones in some states[30]—are, in isolation, not a strong indicator of identity. There is a reason one needs to present multiple forms of identification. Moreover, particularly for digital credentials, copying and sharing are potential problems. As a result, the practical usage of verifiable digital credentials will require multiple trust signals that go well beyond a simple credential. This may be as simple as a trusted platform (e.g., as provided by a mobile phone manufacturer) or a collection of many different identity signals.

Therefore, while VDCs can technically operate without zero knowledge proofs, multi-party compute, or open blockchain networks, it's only through the combination of these technologies that we can meaningfully improve digital identity. In the next subsection (III.B), we'll discuss how sharing a credential without zero-knowledge proofs could reveal more personal

[29] ACLU Digital ID State Legislative Recommendations, https://assets.aclu.org/live/uploads/2024/10/ACLU-Digital-ID-State-Legislative-Recommendations-version-1.0-October-2024-1.pdf (last visited Aug 12, 2025).
[30] Mobile ID World, Three U.S. States to Launch Mobile Driver's Licenses in 2025, https://mobileidworld.com/three-u-s-states-to-launch-mobile-drivers-licenses-in-2025/ (last visited July 1, 2025).

information than is necessary, compromising privacy. In Section III.C, we'll focus on how sharing and aggregating VDCs without open blockchain networks introduces risks and costs: it becomes difficult to manage credential revocation, ensure issuer key transparency, or enable portable, cross-domain trust. Open blockchains address these gaps by providing a neutral, tamper-evident layer for anchoring the status and metadata of credentials and for aggregating those credentials into dynamic risk scores without relying on centralized authorities.

B. Zero-Knowledge Proofs and Multi-Party Computation: Proving Facts Without Revealing Credentials

Verifiable digital credentials give users control over their identity data—but without the right cryptographic tools, even sharing a credential can mean revealing too much. That's where zero-knowledge proofs (ZKPs) and secure multi-party computation (MPC) come in. These techniques allow users to prove that they meet a requirement—such as being over 18, not appearing on a sanctions list, or holding a credential from a trusted issuer—without revealing the credential itself or any other underlying information.

A zero-knowledge proof is a mathematical method that allows someone to prove that a statement is true without showing *why* it's true. In the context of digital identity, that means proving something about the contents of a VDC—such as a user's age, jurisdiction, or risk score—without revealing the VDC itself or the user's personal information. For example, instead of sharing a full date of birth, a user can generate a zero-knowledge proof that they are over 21. Or, instead of disclosing their name and passport number, a user can prove that they have been cleared through a government-run sanctions list check. These technologies make possible the move from identity verification to attribute verification discussed earlier, and they simultaneously support our principle of surveillance resistance.

Secure multi-party computation (MPC) addresses a different but related problem: allowing multiple parties to jointly compute something using their private inputs, without exposing those inputs to each other. In a credential system, MPC could be used by several institutions to assess a user's fraud risk or perform an eligibility check, combining their data in a way that's useful to the verifier but private to all participants. Banks or exchanges, for example, could compute a cryptographic "risk rating" based on their own internal flags, without revealing individual data points or customer history to the public, the government, or their competitors.

These privacy-preserving techniques enable a shift from traditional KYC processes—which involve collecting, storing, and auditing large volumes of personal data—to a system where proofs, not documents, are exchanged, where personal attributes or risks scores matter more than personal identity or names, and where compliance can be demonstrated without mass surveillance. It also (1) mitigates over-collection of data, (2) reduces breach exposure, and (3)

allows use of credentials across borders without needing every jurisdiction to adopt identical databases. What matters is that the proof is valid, not that the credential is identical.

Real-world implementations of these tools are already live or in advanced stages of development.[31] These tools are not theoretical—they are increasingly practical, scalable, and efficient. They allow individuals to use their VDCs to answer sensitive questions without giving up control of their data. And they allow verifiers to trust those answers without needing to surveil the user or replicate the original verification process.

C. Open Blockchains: Anchoring and Aggregating Trust Without Centralized Control

Verifiable digital credentials (VDCs) give you control over your digital identity. Zero-knowledge proofs (ZKPs) and secure multi-party computation (MPC) let you prove facts derived from those credentials without revealing the underlying data. Together, they form a foundation for user-centric, privacy-preserving verification. But in practice, identity is rarely a single, static fact. It is dynamic, layered, and contextual. To handle that complexity, we need not just private credentials—we need a neutral arena where credentials, proofs, and participants can interact. This is where open blockchains come in.

Digital identity exists on a spectrum of complexity:

- **Basic Verification:** Proving a simple fact, like "I am over 21" or "I am not a resident of a sanctioned country." A ZKP derived from a single VDC might suffice.

[31] Projects like zPass (built on Aleo) allow users to generate anonymous proofs of attributes derived from traditional ID documents, without disclosing the documents themselves. See Aleo, Introducing zPass: Aleo's Pioneering Step Toward Privacy-Preserving Digital Identity (Oct. 2023), https://aleo.org/post/introducing-zpass-aleos-pioneering-step-toward-privacy-preserving-digital. Aleo is live today and developers are experimenting with identity tools as well as other privacy-focused applications. Other networks are coming online, Aztec and Polygon Miden are building privacy-focused, zk-rollup systems on top of Ethereum that could provide scalable and private execution environments for identity proofs and selective disclosure applications. See Polygon Miden Documentation, https://0xpolygonmiden.github.io/miden-docs/ (last visited Apr. 25, 2025). Aztec Labs, What Is Noir?, https://docs.aztec.network/noir/overview. Anoma is developing decentralized infrastructure that enables private coordination and encrypted settlement between users and between blockchains without reliance on centralized intermediaries. See Adrian Brink et al., Anoma: An Intent-Centric Privacy-Preserving Protocol for Decentralized Counterparty Discovery and Settlement (2024), https://anoma.net/whitepaper.pdf. In the institutional world, MPC is already widely used in digital asset custody systems and is being integrated into risk computation and fraud detection tools. See Yehuda Lindell, Secure Multiparty Computation for Privacy-Preserving Data Analysis, 68 Commun. ACM 86 (2023); Fireblocks, Multi-Party Computation (MPC) Explained, https://www.fireblocks.com/blog/what-is-mpc/.

- **Multi-Factor Identity:** Gaining higher assurance by combining several signals—for example, a government-issued ID, control of a trusted device, and a verified relationship with a financial institution.

- **Identity as Reputation:** The most sophisticated use case, involving dynamic, updatable scores—such as a real-time AML or fraud risk score based on private transaction history and group attestations like "this name is not on a blocklist."

As we move up this spectrum, a key challenge emerges: who combines these signals, and how? The system must allow for flexible, dynamic aggregation—but also protect user autonomy. This creates a fork in the road.

One path leads to new *Walled Garden*s. A centralized intermediary—Apple, Google, a bank consortium, even a government agency—ingests various credentials, runs proprietary algorithms, and returns a simple "verified" stamp. While convenient and efficient, this model makes one entity the arbiter of trust, able to privilege its own services, limit interoperability, or deny access based on opaque criteria. It replicates the problems of the current financial identity regime: centralization, surveillance, and control.

The other path leads to an *Open Commons*: a public infrastructure where credentials can be issued, combined, verified, and revoked according to shared, transparent rules—without a central gatekeeper. This is where open blockchains offer critical leverage. Not as a storage layer for sensitive data, but as a neutral coordination layer: a place to register identifiers, anchor credential metadata, and enforce rules about how identity components can be updated, combined, and trusted.

Open and programmable infrastructure enables more than static identity—it enables privacy-preserving computation of risk, eligibility, or reputation. For example, a blockchain protocol might define: "Build risk score X if and only if user Y authorizes institutions A, B, and C to participate in a secure multi-party computation." Each institution contributes encrypted data, the output is encrypted and shared only with authorized recipients, and no participant learns more than they contributed. The result is provably correct and minimally invasive.

This structure enables not just transparency but adaptability. Identity systems must evolve to meet changing fraud tactics. Scoring architectures should support rapid updates to inputs and weights—what military planners call an OODA loop: Observe, Orient, Decide, Act. A score might draw from a state-issued ID (proving jurisdiction), Gmail history (proving longevity), or on-chain assets (proving non-association with hacks or sanctions). If any one input is compromised—say, a DMV breach or email spoofing exploit—the system must adapt without loss of integrity.

But adaptability cuts both ways. The most agile scoring system is one where a single entity has all the inputs and full control over the weights. That may be effective—but it's also profoundly dangerous. It concentrates sensitive data, invites abuse, and removes user agency. This is the tradeoff at the heart of modern identity infrastructure: how to stay agile without building new chokepoints.

Open blockchains **mitigate** this tension by shifting the locus of control to the individual. They provide a framework where users themselves decide how to combine their identity signals according to **public, auditable rules**. Because these computations are **user-initiated**, no single entity needs to hold all the data or make all the decisions. This creates a foundation that is resilient, composable, and censorship-resistant by its very design

This is how we realize the three paradigm shifts described earlier: from siloed documentation to portable credentials, from identities to attributes, and from static forms to dynamic proofs. It's also how we operationalize the seven principles that should guide digital identity: user control, surveillance resistance, censorship resistance, breach resistance, network privacy, offline capability, and recovery resilience.

An open commons approach is not just technically sound—it is politically necessary. Under our federalist system, states retain significant power over identity-related credentials: licenses, permits, certifications. That diversity enables state-by-state experimentation but hampers coordination. Suppose two states wish to recognize each other's professional licenses or concealed carry permits. Do they each need to build a new integration layer—or appeal to a federal agency to intermediate trust? No. They need a shared protocol and a neutral verification layer. Open standards and open infrastructure can do the job without sacrificing sovereignty.

Ultimately, it doesn't matter which blockchain or vendor wins. What matters is that the system guarantees key properties: auditability without centralized control, strong privacy by default, and compatibility with open identifiers. Whether implemented on a public chain, a privacy-preserving rollup, or a future cryptographic substrate, identity infrastructure should serve users, not platforms.

V. Digital Identity as Public Good: The Case for Limited Government Action

After reading the previous section you might be thinking, '*This all seems very complex. Wouldn't it be better to just let the private sector handle everything?'* After all, competition drives innovation, and governments rarely excel at providing goods and services that lie anywhere near the bleeding technological edge. But digital identity infrastructure is not a typical private good. It has the structural features of a public good: its value depends on broad adoption,

interoperability, and shared trust frameworks that no single actor has sufficient incentive to build alone. Without deliberate coordination, several bad outcomes loom: *fragmentation* (each bank or government siloing its own credentials), *monopolization* (a few big internet platforms controlling identity and extracting rents), or a continuation of today's *surveillance-driven model* (perhaps with big tech companies rather than banks playing the role of state surveillance deputy). Down these paths lie a betrayal of the principles for digital identity that we explained earlier: instead of breach resistance we get honeypots, instead of user control we get backdoors, instead of censorship resistance — chokepoints.

The core technologies to support a better system—verifiable digital credentials (VDCs), zero-knowledge proofs (ZKPs), secure multi-party computation (MPC), and open blockchains—are ready. But identity infrastructure is more than a technological problem. It is also a coordination problem, and one with the economic characteristics of a public good: non-rivalrous, network-dependent, and prone to underinvestment without shared incentives or governance. Its value depends on adoption by many users, issuers, and verifiers. Without coordination, the system fragments. Each bank, government, or enterprise may create its own credential format, its own revocation registry, its own trusted list of issuers. Users may find that their credentials are accepted in some places but not others. Verifiers may struggle to assess the trustworthiness of unfamiliar credentials or be forced to replicate compliance burdens across incompatible systems.

This is a textbook case of collective action failure. Everyone benefits from an open, interoperable identity ecosystem, but no single actor has sufficient incentive to bear the upfront costs of building it. Issuers are reluctant to invest in new credential systems unless enough verifiers exist to accept them. Verifiers are reluctant to trust new systems unless enough issuers adopt common standards. Users are reluctant to rely on credentials that may not be recognized universally.

In theory, market competition alone could eventually converge on a few dominant credential providers. But history shows that without intervention, such convergence often leads to centralization, rent extraction, and the degradation of individual rights. The early days of the internet saw similar dynamics: closed online services like AOL and CompuServe initially thrived by building walled gardens, while open protocols like TCP/IP and HTTP struggled to gain traction. Only deliberate public support for open standards—and resistance to premature monopolization—allowed the open internet to emerge as the foundation of today's global communications network. The Clinton Administration strongly supported open internet architecture in the 1990s, calling for private sector leadership in standard setting and a limited role for government:

> Where government intervention is necessary to facilitate electronic commerce, its goal should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions, and facilitate dispute resolution.[32]

Today, digital identity faces a similar crossroads. Without clear standards and incentives for openness, the future may belong to a handful of powerful identity providers: social media giants, financial conglomerates, or government agencies operating closed systems. These entities could entrench surveillance, restrict user mobility, and extract monopolistic rents from a captive user base. A decentralized, privacy-respecting alternative will not emerge spontaneously. It must be seeded and protected, much as the early internet was.

Government action can play a critical role just as it did with the early internet—not by building or controlling the infrastructure itself, a state-run walled garden is no better than a private park, but by encouraging open standards, certifying compliance, and creating legal safe harbors for institutions and developers who adopt or build privacy-preserving credential systems. The goal is not to replace market competition, but to catalyze it in the direction of openness, interoperability, and individual privacy and autonomy—ensuring that public goods are properly provisioned rather than captured by private monopolies.

As with the early internet, Government is well positioned to seed demand for better digital identity—but it is poorly equipped to design the supply side. Regulators like the Department of the Treasury and the Securities Exchange Commission do not have the in-house expertise to define rigorous, state-of-the-art standards for decentralized credentials, zero-knowledge proofs, selective disclosure, and revocation registries. These technologies are advancing rapidly in the open-source and cryptography communities, not in Washington. If pilot programs are to succeed, they must be able to rely on technical architectures that are robust, privacy-preserving, and open—not cobbled together in-house or contracted out to legacy vendors.

That's where open, voluntary coordination by the private sector becomes essential. Imagine a stakeholder group—tentatively called the John Hancock Project (JHP)[33]—composed of

---

[32] A Framework for Global Electronic Commerce, The White House (July 1, 1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

[33] John Hancock signed the Declaration of Independence so boldly that his name became a shorthand for every American's signature. In the 21st century, faced with ubiquitous surveillance and the renewed specter of state control over our lives—our bank accounts, our speech, our very identities online—we call for new, bottom-up, open-source identity and privacy technologies. Tools anyone can use, and no one can control. These are the technologies that can secure our constitutional values for another 250 years.

privacy-focused technologists, civil liberties advocates, and academic experts. The JHP could develop open standards for decentralized, maximally privacy-preserving identity credential architecture and urge Congress and regulators to authorize regulated providers to rely on them.

JHP would not begin with government direction or funding. It would emerge from the recognition that the future of digital identity must be both technically excellent and aligned with American values. Many of its potential participants already exist: developers working on zero-knowledge cryptocurrency L1s and L2s; teams building non-custodial (user-controlled) cryptocurrency software and hardware wallets; public interest organizations like Coin Center, the ACLU, or the Electronic Frontier Foundation; and researchers in cryptography and privacy engineering at leading universities.

These stakeholders are already building and auditing the pieces of a better identity infrastructure. What's missing is a neutral, transparent venue for aligning their efforts, validating them with third parties, and packaging the results into something regulators and institutions can safely adopt.

That's the role JHP would play. Its mission would be to:

- Draft and maintain open technical standards for verifiable credentials, decentralized identifiers, revocation, and privacy-preserving proofs;
- Ensure those standards are modular, testable, and auditable so a wide range of actors can implement them;
- Build in third-party validation by civil-liberties organizations to guard against surveillance creep and centralized control;
- Incorporate peer-reviewed academic input to ground the work in state-of-the-art cryptography and threat modeling; and
- Prepare deployment profiles for regulated services and secure legislative and regulatory recognition so regulated providers can—indeed should—adopt decentralized, privacy-preserving digital identity methods.

The outcome would be a set of open, trustworthy technical baselines that government pilot programs could reference directly, reducing duplication and lowering barriers to adoption. Regulators would remain in control of compliance policy—but they wouldn't be left guessing about what technical architecture for compliance is safe, effective, and civil-liberties-aligned.

JHP is not meant to compete with every existing digital-ID consortium or to become an all-things-to-all-people governance body. As we imagine it, JHP's mandate would be deliberately narrow and agile: convene a small, already engaged cohort of privacy-minded crypto projects—where private, decentralized ledgers have reached real technical

maturity—and pair them with civil-libertarian watchdogs and academic cryptographers. By keeping the table compact, JHP can iterate quickly, perhaps avoiding the politics that bog down broader identity forums, and deliver a privacy-maximizing baseline that is immediately scalable, regulator-ready, and simple for others to build on—just as the internet grew from a handful of lean, interoperable protocols rather than a monolithic standard.

The result: when the government acts—as it must, to unlock network effects through pilot programs and, eventually, regulatory changes—it will find that the hard part is already done. Viable architecture will be waiting. The values will be embedded. All it will need to do is point to what already exists—and begin.

VI. Federal Action to Seed Open Identity Infrastructure in Five Steps

The market will not build open, privacy-preserving identity systems on its own. But that does not mean the government must build them either. What is needed is a limited but proactive role: to encourage open technical standards, certify compliance, create clear legal pathways for adoption, protect the builders of critical infrastructure, and promote the long-term minimization of personal data collection. The task is not to pick winners, control networks, or impose centralized mandates. It is simply to ensure that decentralized, user-respecting systems have a real chance to emerge and compete.

Seeding open identity infrastructure will require deliberate government action. That action can proceed along two complementary paths: a lightweight regulatory approach using existing statutory authority, and a full legislative framework to permanently establish the system in law. Both paths must address all five pillars outlined below: standardization, certification, mandated acceptance and safe harbors, protection of infrastructure developers, and credential minimization over time. In this section, we will briefly outline those pillars and summarize steps that can be taken today by agencies using existing authority, as well as how Congress can ultimately concretize these policies.

1. Open Technical Standards

The first step toward an open identity ecosystem is the establishment of shared technical standards. But these standards should not be written by a single agency in Washington. They should emerge from open, collaborative efforts grounded in both cryptographic research and civil liberties.

We propose that regulators look to a proposed John Hancock Project (JHP)—a voluntary, multi-stakeholder body of privacy-focused technologists, civil liberties advocates, and academic experts—as an engine for standard development. JHP would publish modular,

auditable specifications for decentralized identity infrastructure, including verifiable credentials, decentralized identifiers (DIDs), revocation mechanisms, and privacy-preserving proofs (e.g., zero-knowledge attestations). These standards would be maintained through transparent processes and benefit from third-party validation by civil liberties organizations and cryptographers.

Regulatory agencies—especially Financial regulators within the Department of the Treasury, SEC, CFTC, and OCC—should monitor and consult with JHP, but not control it. The goal is to ensure that government adoption, when it comes, builds upon an architecture that is technically sound, maximally privacy-protective, and resilient to capture. Pilot programs, certification frameworks, and eventual rulemaking efforts should be interoperable with JHP-compliant standards from day one.

FinCEN within the Treasury already has a natural forum for dialogue on these topics. Its September 2021 "Innovation Hours" workshop on privacy-enhancing technologies paired agency examiners with technologists for structured sessions, however the program appears dormant today.[34] FinCEN should restart those hours on a recurring schedule and invite JHP—or any comparable open-standards body focused on privacy and identity—to present standard setting and certification work.

Sanctions compliance deserves equal attention. The Office of Foreign Assets Control within Treasury, (OFAC) has not yet hosted a workshop on zero-knowledge or selective-disclosure proofs, but its 2019 *Framework for Sanctions Compliance Programs* encourages financial institutions to deploy advanced screening technologies and to "continuously test and improve" analytic methods.[35] Linking OFAC staff into a revived FinCEN Innovation Hours session would create the venue to demonstrate how a JHP-compliant credential can prove a user is *not* on the SDN list without revealing any additional identity data.

The Securities and Exchange Commission has similar mechanisms for private sector consultation: its new Crypto Task Force, working alongside the long-standing FinHub office-hours channel, provides an obvious venue for identity projects that intersect securities law.[36] The SEC has recently signaled its interest not only in novel digital identity systems but

[34] Financial Crimes Enforcement Network, *FinCEN to Host Innovation Hours Program Workshop on Privacy-Enhancing Technologies* (Sept. 9, 2021), https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-privacy-enhancing-technologies.
[35] Office of Foreign Assets Control, A Framework for OFAC Compliance Commitments (May 2, 2019).
[36] U.S. Securities & Exchange Commission, *Crypto Task Force* (visited June 2025), https://www.sec.gov/about/crypto-task-force; SEC, *Strategic Hub for Innovation and Financial Technology (FinHub)*, https://www.sec.gov/finhub.

also the restoration of financial privacy generally. As Commissioner Peirce remarked in a recent speech,

> We should take concrete steps to protect people's ability not only to communicate privately, but to transfer value privately, as they could have done with physical coins in the days in which the Fourth Amendment was crafted.
>
> Most fears of financial privacy and the technology that enables it flow from a genuine desire to protect this nation from enemies and criminals. Safeguarding our families, communities, and country from harm is extremely important, but curtailing financial privacy and impeding disintermediating technologies are the wrong approach. Denying people financial privacy—whether through sweeping surveillance programs or restrictions on privacy-protecting technologies—undermines the fabric and freedoms of our families, communities, and nation. The American people and their government should guard zealously people's right to live private lives and to use technologies that enable them to do so.

Only the technologies discussed in this report can enhance Americans' privacy while preserving auditability and risk-based oversight needed to meet legitimate regulatory objectives at the SEC and at other agencies.

The National Institute of Standards and Technology (NIST), for its part, has long shaped federal e-authentication policy through its *Digital Identity Guidelines* (SP 800-63) and convenes public workshops when revisions are underway. Revision 4, released August 1st, 2025 (SP 800-63-4), explicitly mentions digital credentials as an acceptable evidence pathway for identity proofing.[37] Due to the relevance of its work in enabling privacy, data security, and compliance, NIST should engage the emerging digital assets industry as an observer and technical critic, ready to translate the lessons that emerge from the JHP, similar initiatives, and potential agency pilots into implementer guidelines and reference architectures as the underlying methods continue to mature.

NIST's Digital Identity Guidelines are already appropriately principles based rather than technology or document specific. Under those guidelines, certain implementations of the above described zero-knowledge proof based identity model could qualify for Identity Assurance Level 2 (IAL2) Requirements. NIST has already worked alongside another public-private partnership, the National Cybersecurity Center of Excellence (NCCoE), to develop the NCCoE Mobile Driver's

[37] National Institute of Standards & Technology, Digital Identity Guidelines, SP 800-63-4, Second Public Draft (Aug. 21, 2024) (public workshop and comment process), https://www.nist.gov/news-events/news/2024/08/nist-sp-800-63-4-digital-identity-guidelines-second-public-draft.

License Program which includes reference architecture for the use of IAL2 at financial services providers for KYC onboarding.

A modest early agenda for the John Hancock Project could be to—first—specify in detail how a zero-knowledge-based credential system could meet various regulatory compliance requirements while maximizing user privacy and autonomy, and—second—advocate with regulators for a pilot program at Financial Institutions that follows the IAL2 proofing processes while utilizing VDCs, privacy-preserving proofs, and blockchains. Additionally, the JHP can work to develop a rubric of proofs and use cases where an individual's full identity need not be verified, but rather some proof of an attribute alone can suffice. As we discuss further in subsection five below, in many cases proofs can be made selectively to show a user's attributes without revealing their full identities, such as a "non-sanctioned entity" or "meets risk-score X." This modern, data-minimized approach is better matched for the digital world, and may result in superior compliance, anti-fraud, and privacy than existing requirements, *e.g.* FinCEN's existing CIP standards.

We are, however, getting ahead of ourselves. The key takeaway is that the first step toward seeding digital identity systems that embody American values of privacy and autonomy is to standardize and describe methods that honor those values. That should be done by the private sector, the JHP among others, in conversation with future potential users and beneficiaries of those standards, regulators and policymakers.

2. Certification of Credential Issuers

A privacy-preserving credential is useful only if a verifier can trust both the cryptography and the compliance practices that stand behind it. That trust is established by certifying the *issuer's program as a whole,* not by rubber-stamping every credential one at a time.

When a supervisory agency is ready to experiment, it should open a bounded pilot that lets regulated firms accept an "alternative identity lane." Wherein regulated firms can onboard users via privacy-preserving credentials or risk scores from certified issuers and/or proof aggregators. Participation would be limited to issuers that clear two sequential reviews:

1. **Independent technical audit.** External assessors—neither the regulator nor the issuer—test the issuer's system against the John Hancock Project (JHP) specification. They confirm that keys are managed correctly, revocations are anchored to a public ledger, and selective-disclosure proofs function as specified.

2. **Supervisory compliance review.** The agency then examines the issuer's policies for customer identification, due diligence, and risk management. The question is

straightforward: do these procedures, taken together, satisfy the legal standard that would otherwise apply if the bank had collected and stored traditional documents?

An issuer that passes both reviews is listed in a public registry. Each registry entry specifies the regulatory weight of the issuer's credentials—for example, "meets baseline Bank Secrecy Act CIP," or "satisfies accredited-investor verification under Rule 501." Within the pilot, a bank or broker-dealer may rely on the credential for exactly the obligation to which it is matched, enjoying safe-harbor protection for good-faith reliance. Regulatory pilots could also work in conjunction with open standards setting bodies like our proposed JHP in order to standardize and set thresholds for aggregated credentials or risk scores. For example, if a potential customer for a financial institution (participating in a pilot program) can present three proofs of US-personhood from three different certified issuers this could lessen the need to collect personal biographical information, or increase the cap under which the customer is able to transact before enhanced due diligence kicks in. To offer another example, perhaps a customer can be kept under some transaction cap, but otherwise be onboarded without any traditional ID documents, instead they would be asked to combine various non-traditional identity attributes in a standardized risk score, e.g. verifiable control over longstanding social media profile at various platforms plus proof of certain on-chain digital asset activities. We may find that these proofs are more robust against fraud while also lowering the costs of onboarding and the resultant impediments to financial inclusion.

Existing Authority: Current statutes already give agencies the discretion they need: FinCEN can approve alternative customer-identification programs, the SEC can grant exemptions for experimental onboarding, and prudential regulators can run sandboxes for safety-and-soundness purposes.

Statutory Enhancement: Over time Congress can convert this agency-by-agency discretionary process into a standing, government-wide accreditation regime—one registry, one open standard, and credentials recognized across agencies—while preserving the twin audits that keep both code and compliance honest.

3. Permitting Acceptance and Creating Legal Safe Harbors

With a certification system in place, regulators can allow acceptance of certified credentials for compliance purposes, first at regulated entities participating in pilot programs and ultimately across the entire regulated sector. Financial institutions and other regulated entities should be allowed to accept a certified credential as sufficient proof of identity, status, or eligibility, provided the credential is relevant to the institution's regulatory obligations.

At the same time, institutions that rely in good faith on a certified credential should be fully shielded from both civil liability and regulatory enforcement actions, absent actual knowledge of fraud.[38] Without clearly permitting acceptance, inertia and uncertainty will preserve the status quo. Without full safe harbor protections, uncertainty will chill adoption.

Federal financial regulators—including the Department of the Treasury, the Securities and Exchange Commission (SEC), and banking regulators—should ultimately issue guidance formalizing these requirements. Pilot programs could be launched to gather operational experience in limited contexts: for example, onboarding for lower-risk customers, cross-border payments, or accredited investor verification. But the existence of pilots should not delay the establishment of a binding duty to accept certified credentials once the standards and certification systems are in place.

Existing Authority: Federal regulators already have the authority to permit alternative compliance pathways and provide liability protection through rulemaking and interpretive guidance. The Financial Crimes Enforcement Network (FinCEN) may specify permissible methods for satisfying Customer Identification Program (CIP) obligations under the Bank Secrecy Act (BSA), and can approve reliance on certified credentials as a valid form of identity verification pursuant to its regulatory authority.[39] FinCEN also wields explicit exemptive authority under the BSA, allowing it to waive or tailor record-keeping and reporting rules for specified persons, transactions, or classes of activity through regulation or administrative order.[40] Similarly, the Securities and Exchange Commission (SEC) has authority under the Securities Act of 1933 to define procedures for verifying accredited investor status[41] and may grant exemptions consistent with the public interest and investor protection.[42] Prudential regulators—including the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation

[38] 31 U.S.C. §§ 5318, 5321 (Bank Secrecy Act obligations); 31 C.F.R. § 1020.220 (customer identification program rules for banks); see also Financial Crimes Enforcement Network (FinCEN), Customer Identification Programs for Financial Institutions, 68 Fed. Reg. 25090 (May 9, 2003).
[39] 31 U.S.C. § 5318(l) (authorizes Treasury to require financial institutions to implement Customer Identification Programs); 31 C.F.R. § 1020.220(a)(2) (bank-CIP rule detailing the procedures a bank must follow to verify each customer's identity).
[40] 31 U.S.C. § 5318(a)(7); 31 C.F.R. § 1010.970 (authorizing the Secretary of the Treasury, acting through FinCEN, to exempt any person, class of persons, transaction, or class of transactions from BSA requirements by regulation or written order).
[41] 15 U.S.C. § 77d(a)(2) (statutory private-offering exemption on which Regulation D is based); JOBS Act § 201(a)(1), Pub. L. No. 112-106, § 201(a), 126 Stat. 306 (2012) (directs SEC to adopt rules requiring "reasonable steps" to verify accredited-investor status), and 17 C.F.R. § 230.506(c)(2)(ii) (implements JOBS Act mandate by specifying permissible verification methods).
[42] 15 U.S.C. § 77z-3 (gives SEC broad authority to exempt any person, security, or transaction from Securities Act requirements when consistent with the public interest and investor protection).

(FDIC)—may incorporate credential acceptance into supervisory guidance under their safety and soundness mandates.[43] These agencies can also initiate pilot programs and regulatory sandboxes under their existing interpretive and supervisory discretion.

Statutory Enhancement: To ensure clarity and permanence across jurisdictions, Congress should amend relevant provisions of the BSA, securities laws, and banking statutes to require regulated entities to accept certified digital credentials as sufficient for specific compliance obligations, subject to regulatory determination of equivalence. These amendments should also establish a statutory safe harbor, shielding institutions from liability (civil or criminal) and enforcement actions when they rely in good faith on credentials issued by certified entities, absent actual knowledge of fraud or misuse.[44] To prevent regulatory fragmentation, Congress can authorize the creation of a unified federal registry of certified credential issuers and direct interagency coordination under the Financial Stability Oversight Council (FSOC).[45] This will ensure consistent treatment of compliant digital identity frameworks across all financial regulatory regimes.

4. Protecting the Builders of Privacy and Identity Infrastructure

Fourth, any serious strategy must protect the developers who create the underlying infrastructure. Credential wallets, decentralized revocation registries, zero-knowledge proof libraries, decentralized identifier resolvers—all of these tools are essential for an open ecosystem.

Developers who build general-purpose privacy tools should not face liability or prosecution merely because their work can be misused. So long as a tool is general-purpose, privacy-preserving, and not designed to facilitate specific unlawful conduct, its publication and maintenance must be affirmatively protected, either by statute or by clear regulatory guidance.[46]

---

[43] See, e.g., 12 U.S.C. § 1831p-1 (requires agencies to prescribe and enforce safety-and-soundness standards for insured depository institutions).

[44] Cf. 31 U.S.C. § 5318(g)(3) (grants immunity for filing Suspicious Activity Reports in good faith); 15 U.S.C. § 77z-2(c) (safe harbor for forward-looking statements under the Securities Act); 15 U.S.C. § 78u-5(c) (parallel forward-looking-statement safe harbor under the Exchange Act).

[45] 12 U.S.C. § 5322(a)(2)(E) (directs FSOC to "facilitate information sharing and coordination" among federal and state financial regulators).

[46] See Indictment, United States v. Storm, No. 1:23-cr-00418 (S.D.N.Y. Aug. 23, 2023) (charging Tornado Cash developer for alleged money laundering facilitation); see also Press Release, U.S. Department of Justice, Founders of Samourai Wallet Arrested for Alleged Money Laundering and Operating an Unlicensed Money Transmitting Business (Apr. 24, 2024), https://www.justice.gov/opa/pr/founders-samourai-wallet-arrested-alleged-money-laundering-and-operating-unlicensed-money.

Without builders, there is no infrastructure. And without legal clarity, only large, centralized platforms will have the resources and risk tolerance to continue innovating. Criminalizing or chilling the development of open identity tools would entrench the very surveillance-first models this effort seeks to avoid.

Developers who create privacy-preserving identity tools face at least five distinct legal threats under current U.S. law:

1. **Liability for operating as an unlicensed money transmitter under 18 U.S.C. § 1960**: In the cryptocurrency context, FinCEN's 2019 guidance properly clarifies that merely developing and publishing non-custodial software—such as wallets, credential clients, or decentralized proof generators—does not constitute money transmission or create a money services business obligation.[47] Nonetheless, the DOJ has aggressively pursued prosecutions against non-custodial developers of privacy tools.[48] Recently the DOJ has suggested it will, in its discretion, avoid continued prosecutions that are counter the FinCEN guidance, but it has not clearly stated that such prosecutions are (or were) outside its statutory jurisdiction (thus reserving the right to restart said prosecutions); additionally, the DOJ now faces a civil suit for declarative judgement on whether their

Cf. Peter Van Valkenburgh, DOJ's New Stance on Crypto Wallets Is a Threat to Liberty and the Rule of Law, Coin Center (Apr. 25, 2024), https://www.coincenter.org/dojs-new-stance-on-crypto-wallets-is-a-threat-to-liberty-and-the-rule-of-law/.

[47] See FinCEN, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 9, 2019). In Lewellen v. Garland, the government faces a civil challenge arguing that non-custodial software development does not violate 18 U.S.C. § 1960.

[48] See Indictment, United States v. Storm, No. 1:23-cr-00418 (S.D.N.Y. Aug. 23, 2023) (charging Tornado Cash developer for alleged money laundering facilitation); see also Press Release, U.S. Department of Justice, Founders of Samourai Wallet Arrested for Alleged Money Laundering and Operating an Unlicensed Money Transmitting Business (Apr. 24, 2024), Cf. Peter Van Valkenburgh, DOJ's New Stance on Crypto Wallets Is a Threat to Liberty and the Rule of Law, Coin Center (Apr. 25, 2024). These prosecutions assert that publishing open-source tools, even without custody or financial intermediation, can constitute illegal transmission. The DOJ's recent memorandum on "Ending Regulation by Prosecution" suggests a promising commitment to respecting agency guidance, but that commitment rang hollow as the charges were not dropped in ongoing prosecutions that ultimately proceeded to guilty verdicts and pleas. Memorandum from the Deputy Attorney General to All Department Employees, *Ending Regulation by Prosecution* (Apr. 7, 2025). In a subsequent speech, Assistant Attorney General Galeotti elaborated, suggesting that new prosecutions for unlicensed money transmission would not be authorized against software developers but legal uncertainty remains.

interpretation of the law is outside the statute and unconstitutional.[49] Binding legal clarity is still needed to ensure that non-custodial developers are not in danger of prosecution for unlicensed conduct.

2. **Criminal aiding and abetting of money laundering under 18 U.S.C. §§ 1956–1957**: Developers face risk under money laundering statutes, based on tenuous theories that building or maintaining a tool that could theoretically be misused constitutes criminal facilitation. Clarification is needed to ensure that liability under money laundering statutes requires proof of purposeful facilitation—not mere awareness that others could misuse a neutral tool.

3. **Liability for sanctions evasion under the International Emergency Economic Powers Act (IEEPA) and OFAC regulations:** Developers risk exposure under sanctions laws. Under current OFAC practices, even purely informational transactions involving sanctioned individuals can trigger scrutiny. The Berman Amendments to IEEPA, however, explicitly protect the dissemination of informational materials, and that protection should be reaffirmed for decentralized identity proofs. Issuing a verifiable credential to a sanctioned person—truthfully documenting their sanctioned status—should not itself constitute a sanctions violation.

4. **Liability for wire fraud:** Developers of privacy-preserving identity tools could face liability under the federal wire fraud statute, 18 U.S.C. § 1343, if prosecutors wrongly argue that their tools "facilitated" a fraudulent scheme.[50]

5. **Liability for Computer Fraud and Abuse Act (CFAA) violations.** Developers might also face risk under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030,

[49] Lewellen v. Garland, No. 4:25-cv-00030-Y (N.D. Tex. filed Jan. 16, 2025). Michael Lewellen wants to publish new cryptocurrency software that he created to coordinate crowdfunding campaigns for charities and other projects, but the DOJ has been criminally prosecuting people for publishing similar cryptocurrency software, calling it unlicensed "money transmitting" under 18 U.S.C. §1960(b)(1)(B). Lewellen seeks binding clarity on whether he would be violating those laws if he published and maintained a website for that software.

[50] For example, if a bad actor used a verifiable credential (VDC) created with a developer's software to falsely claim eligibility for a service—such as misrepresenting age, nationality, or OFAC status—a zealous prosecutor might allege that the developer "knowingly" enabled wire fraud. Even absent any knowledge or intent on the developer's part, the government might assert that building general-purpose credentialing software constitutes participation in a fraudulent scheme if the tool was foreseeably misused. This mirrors overbroad theories of wire fraud liability that have been criticized in the technology sector before (e.g., United States v. Drew).

particularly if their tools facilitate credential verification processes that interact with third-party servers.[51]

These risks to developers can be addressed by the executive branch—using existing statutory authority—and by Congress amending the underlying criminal code.

Existing Authority: The Department of Justice and the Office of Legal Counsel should issue a formal and binding interpretation of the laws discussed above, explaining that mere developers of general-purpose, non-custodial digital identity and privacy infrastructure are not subject to prosecution under money transmission or laundering statutes, sanctions laws, wire fraud, or the Computer Fraud and Abuse Act (CFAA) absent proof of specific, purposeful facilitation of unlawful conduct. The mere creation, publication, or maintenance of tools that could be misused by third parties must not be grounds for liability. Prosecutors should require clear evidence that a developer knowingly and intentionally designed their tools to further specific illegal transactions (rather than having a vague knowledge that their public tools could be misused), specific sanctions evasions, fraudulent schemes, or unauthorized access to protected systems. Routine, good-faith interaction with public or quasi-public data resources, and the issuance of truthful identity credentials—even to sanctioned persons—should be categorically excluded from criminal liability.

Statutory Enhancement:

Congress should act to:

- **Unlicensed Money Transmission:** Codify that non-custodial software publishing does not constitute money transmission absent custody of funds;
- **Money Laundering:** Clarify that aiding and abetting money laundering liability requires purposeful facilitation, not mere knowledge of possible misuse;
- **Sanctions:** Reaffirm that providing credentials or proofs—even to sanctioned persons—is protected under the Berman Amendments;
- **Wire Fraud:** Congress should amend 18 U.S.C. § 1343 to clarify that liability for wire fraud requires proof that the defendant knowingly and purposefully participated in a

[51] For example, some decentralized identity wallets and credentialing systems need to query revocation registries, metadata repositories, or issuer public key servers. If a user presents a fraudulent credential that allows unauthorized access to a server (e.g., bypassing an access control or authorization gate), prosecutors could attempt to argue that the developer of the verification tool "aided and abetted" unauthorized access—even if the tool was designed for lawful, legitimate verification.
Similarly, if software scrapes or reads publicly available but technically access-restricted data to verify a credential, an aggressive interpretation of "exceeding authorized access" under CFAA could theoretically be applied.

specific fraudulent scheme, and that developing or publishing general-purpose software is not, by itself, sufficient to establish such participation.

- **CFAA:** Congress should amend 18 U.S.C. § 1030 to specify that developing, distributing, or using software to access publicly available or quasi-public data does not constitute unauthorized access, unless the software is specifically designed to circumvent technical access restrictions in violation of clearly communicated terms.
- **General Safe Harbor:** Rather than taking a piecemeal approach to these and other criminal statutes Congress could adopt a safe harbor model that protects the developers from any vicarious liability from criminal usage of their tools whenever the developer lacked specific knowledge and intent to further the criminal act. An excellent model for this approach in the context of traditional cryptocurrency wallet developer liability is the Blockchain Regulatory Certainty Act.[52]

Without these reforms, innovation in identity and privacy could stagnate, and centralized surveillance architectures would dominate by default.

5. Data Minimization and the Evolution of Compliance

Finally, policymakers must recognize that the end goal is not merely portable compliance—it is dynamic data-minimized compliance. Today, even forward-looking digital credentials may carry more information than necessary: names, addresses, dates of birth, full citizenship data. But in a mature verifiable credential ecosystem, financial institutions and regulators should move toward demanding only what is strictly needed for a lawful transaction.

If a user can cryptographically prove that they are not on a sanctions list, that they are above a certain age, or that they satisfy a defined risk profile, then requiring disclosure of their full identity serves no prudential purpose. It exposes users to unnecessary risks of surveillance, discrimination, and abuse. Compliance should mean proving eligibility—not surrendering one's life story.

In the short run, portable credentials already separate authorization from identification more cleanly than current systems. They allow users to move between services without creating new honeypots of sensitive data. But in the long run, credential minimization can become a structural feature of compliance itself: a new default that limits data collection to what is genuinely necessary. A financial institution may have a good business reason to know certain specific risks a customer presents (creditworthiness, illicit activities). That does not mean they have a good business reason to know anything else about them. Indeed, in a free society, we

[52] Blockchain Regulatory Certainty Act, H.R. 1414, 118th Cong. (2023).

should actively seek to deprive financial institutions of any knowledge of our politics, race, sexual preferences, religion, speech activities, etc.

Not all use cases require a fully resolved "foundational identity," and in many cases attribute verification or "functional identity" is the most appropriate approach.[53] In many cases we should prefer proofs of discrete facts to the unnecessary collection of full identities and documents. Notably, this principle of information minimization is already enshrined in NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII):

> Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.[54]

Regulators should plan for this transition. Standards for financial compliance, identity verification, and risk management should evolve alongside credential technologies, moving steadily toward a world where proving a right does not require exposing a person.

Existing Authority:

Regulators already have discretion to support credential minimization. FinCEN and other agencies routinely promote risk-based approaches, which could allow sandbox participants to rely on minimal proofs—such as risk scores or zero-knowledge attestations—instead of full biographic disclosures.

Statutory Enhancement:

Congress can encourage credential minimization first by directing and funding regulators to develop pilot programs for customer onboarding that employ least-privilege data practices. Regulatory agencies, like FinCEN and the SEC, need and deserve room in their budgets to experiment with digital identity programs that would better protect the privacy and freedom of Americans. In the longer run, however, Congress should revise the substantive statutes that have created these data vulnerabilities, such as the Bank Secrecy Act, to permanently shift the regulatory and law enforcement paradigm away from mass data collection.

As Congress revisits financial privacy—often through a Gramm–Leach–Bliley (GLBA) lens of disclosure, sharing limits, and breach notifications—it should also address the upstream cause of today's risks: how much sensitive information banks are required to collect and retain in the

---

[53] World Bank, Principles on Identification for Sustainable Development (Feb., 2021), https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[54] National Institute of Standards & Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), SP 800-122 (Apr. 6, 2010), https://csrc.nist.gov/pubs/sp/800/122/final

first place. Large, regulator-mandated data troves are attractive targets for hackers and convenient reservoirs for warrantless or overbroad government access via deputized compliance. Rules for secure handling are necessary, but the safer policy is to avoid creating the hazard. Think hazardous-waste policy: cleanup is good, preventing waste is better. A modern data-minimization standard would anchor collection and retention in true business necessity, set short default retention periods, and permit privacy-preserving attestations or reasonably calibrated risk scores in lieu of stockpiling raw identifiers and activity logs—so institutions can know what they need to know without seeing everything.

That approach also helps correct a constitutional mismatch created by decades of third-party doctrine. After the Supreme Court upheld BSA recordkeeping in California Bankers Ass'n v. Shultz, the public learned that Fourth Amendment limits would not restrain mandated banking searches, and United States v. Miller confirmed customers lacked a constitutional privacy interest in bank records.[55] The digital era has outgrown those assumptions. In Carpenter v. United States, the Court recognized that at least some searches of exhaustive, involuntary dossiers held by third parties should require a warrant.[56] Congress should build on that momentum: reform the BSA to pare back compulsory collection to what is demonstrably useful for preventing serious crime; sunset and periodically review data-collection obligations; impose strict retention limits; and clarify that records not created for a legitimate business purpose—or not voluntarily provided by the customer—receive Fourth Amendment protection absent a warrant. Pairing revived constitutional protections with true data minimization is the most durable way to deliver financial privacy and security for all Americans.

Executed carefully, these five public policy steps would not replace the private sector. They would unleash it. They would create the conditions under which credential issuers, proof providers, and users could build a decentralized, privacy-preserving identity ecosystem—one that honors American values of individual liberty, due process, and open competition. None of this will happen on its own. Open infrastructure must be seeded deliberately. Now is the time.

VII. Conclusion

The future of digital identity is being written now. If the United States fails to act, it will not mean the problem goes away—it will mean someone else writes the rules. That future may be shaped by dominant platforms pursuing surveillance-driven efficiencies, or by foreign governments embedding authoritarian values into digital infrastructure.

[55] 416 U.S. 21 (1974); 425 U.S. 435 (1976)
[56] 138 S. Ct. 2206 (2018)

But there is another path: one in which individuals control their identity credentials as easily as they carry a wallet. One in which verifiers ask only the questions they are legally entitled to ask, and learn only the answers they are entitled to know. One in which regulators achieve their policy goals—not through dragnet surveillance, but through precise, cryptographically sound attestations.

This path is not hypothetical. The core technologies exist. Verifiable digital credentials, zero-knowledge proofs, secure multi-party compute, and decentralized ledgers can deliver both regulatory compliance and personal freedom. What's missing is coordination—and leadership.

America has been here before. In the early days of the internet, it was not inevitable that open protocols would win. Closed networks like AOL and CompuServe had the resources and the momentum. But deliberate choices—like supporting TCP/IP and the World Wide Web—tilted the playing field toward openness, interoperability, and user agency.[57] Those choices paid off. They made the open internet possible and made it, fundamentally, a uniquely American technological breakthrough.

We face a similar moment now. Identity infrastructure will be built. The question is whether it will be centralized or decentralized, extractive or empowering, surveillant or sovereign. Will digital identity systems honor our American identity: the frontier's openness and the constitution's reverence for individual speech and privacy?

This report has outlined a plan to tip the balance in favor of open systems that will buttress our rights. It has shown that the government need not own the infrastructure or control the networks. It need only do what it does best when it is at its best: set the standards, protect the builders, and get out of the way.

[57] A Framework for Global Electronic Commerce, The White House (July 1, 1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

Appendix 1: Sample John Hancock Project Standards

Note: This sample standard is a highly preliminary starting point for discussion purposes only.

Preamble:

This publication provides guidance for organizations building or operating digital identity systems, including financial institutions, technology providers, regulatory authorities, and credential issuers. By adhering to this framework, organizations can establish privacy-enhancing, interoperable digital identity systems aligned with American values and global best practices. This document supports compliance, encourages innovation, and ensures identity infrastructure remains decentralized, verifiably neutral, and user-controlled.

1. Purpose and Scope

This publication establishes an open, interoperable standard for digital identity credentials, allowing individuals to present cryptographic proofs of identity, eligibility, compliance status, or specific personal attributes without unnecessary disclosure of private information. It defines minimum capabilities required of compliant systems, enabling regulatory compliance (including KYC, AML, accreditation, age verification) while protecting user privacy, autonomy, and control over personal data.

2. Principles

Seven principles undergird and direct all standards herein described. These principles align with JHP's mission to develop a maximally-privacy preserving, censorship resistant identity protocol that enshrines American values of individual privacy, liberty, autonomy, and dignity.

8. **User-Centric Control:** Participation must always be voluntary. A person's autonomy to carry, present, or aggregate credentials should be guaranteed by cryptographic design—not merely by policy promises or institutional goodwill.
   No back door.

9. **Surveillance Resistance:** Neither issuers, verifiers, nor other third parties should be able to reconstruct or observe an individual's credential transaction graph. Privacy should be structurally embedded, preventing passive or active surveillance.
   No phone home.

10. **Censorship Resistance:** Credential holders must be free to use their credentials at will. Apart from legitimate revocation by the issuer, no party should be able to block or prevent a credential from being proved or accepted.
    No chokepoint.

11. **Breach Resistance:** The system should avoid single points of failure. No centralized server—whether controlled by an issuer, verifier, or even the user—should represent a vulnerability for mass credential theft, censorship, or tracking.
    No honeypot.

12. **Network-Level Privacy:** Communications surrounding credential issuance and presentation must protect against metadata leakage, including network-level observers.
    No leaks.

13. **Offline Capability:** Credentials should remain provable and verifiable even without continuous internet access, ensuring resilience in adverse conditions.
    No dead zones.

14. **Resilient Recovery:** Standards should specify secure, transparent self-recovery and multi-party recovery methods to guard against device loss, credential lockout, or key compromise.
    No lockout.

4. Definitions and Roles

- **Issuer**: The entity generating and cryptographically signing credentials attesting to certain facts about an individual or entity.
- **Holder**: The individual or entity possessing and controlling their credentials, stored in personal wallets or identity agents.
- **Verifier**: An entity receiving credentials or cryptographic proofs and validating their authenticity and integrity for compliance or access control purposes.

5. Technical Requirements

5.1 Credential Format and Interoperability

- Credentials **MUST** conform to the W3C Verifiable Credentials Data Model v2.0.
- Credentials **MUST** utilize an extensible, structured data format such as JSON-LD.
- Credentials **MUST** be digitally signed using approved cryptographic algorithms.

5.2 Decentralized Identifiers and Resolution

- Systems **MUST** utilize Decentralized Identifiers (DIDs) resolvable through DID Methods registered with W3C.
- DID documents **MUST** be anchored to open, decentralized registries implemented via censorship-resistant, peer-to-peer ledgers or comparable decentralized data structures. Acceptable implementations include distributed ledgers, blockchains, decentralized hash-trees, or similar auditable, tamper-evident records.
- DID resolution **MUST NOT** rely on any single centralized authority or infrastructure component.

5.3 Credential Revocation and Metadata Anchoring

- Credential revocation information **MUST** be anchored on censorship-resistant, peer-to-peer ledgers or decentralized data structures. Acceptable technologies include blockchains, distributed ledgers, Merkle-based cryptographic accumulators, or equivalent decentralized structures providing cryptographic proof of integrity and availability.
- Revocation mechanisms **MUST** provide strong guarantees against censorship and unilateral alteration by any central party.

5.4 Privacy, Data Minimization, and Selective Disclosure

- Credential holders **MUST** have the capability to selectively disclose only the minimal information required for verification requests.
- Selective disclosure methods **SHOULD** employ privacy-preserving cryptographic proofs, including but not limited to BBS+ signatures, zero-knowledge proofs (zk-SNARKs, zk-STARKs, Bulletproofs), or other approved privacy-preserving methods.
- Credential schemas **MUST** be publicly accessible, documented, and auditable, to allow transparent evaluation by regulators and users alike.

5.5 Offline Verification Capability

- Verifiers **SHOULD** be able to verify credentials or cryptographic proofs without direct or synchronous communication with the issuer, except as specifically required by certain regulatory scenarios.

6. Certification Requirements

To receive certification under the ODIC Framework, credential systems **MUST** demonstrate:

- Compliance with credential formatting and DID standards.
- Implementation of at least one approved selective disclosure or zero-knowledge proof method.
- Use of decentralized, censorship-resistant ledgers or data structures for DID and revocation management.
- Commitment to ongoing interoperability testing with other compliant systems.
- Data handling practices consistent with the principles of minimal disclosure and least privilege.

7. Legal and Regulatory Considerations

- Credentials certified under this standard are designed to meet statutory and regulatory compliance obligations (e.g., Bank Secrecy Act, Securities Exchange Act, sanctions screening) without excessive personal data exposure.
- Regulatory agencies **SHOULD** recognize certified credentials and proofs as legally sufficient evidence for compliance, where applicable.
- The creation, publishing, or distribution of credential infrastructure and related software components **SHALL NOT**, by itself, constitute regulated financial activities such as money transmission, money laundering, or violation of economic sanctions.

8. Future-Proofing and Adaptability

This standard anticipates future cryptographic developments and regulatory shifts. Future versions **MAY** incorporate advances such as:

- Post-quantum cryptographic primitives.
- Enhanced privacy-preserving revocation mechanisms.
- Expanded DID resolution methods and decentralized registry technologies.

9. Implementation and Operational Considerations

- Credential issuers and verifiers **SHOULD** clearly document implementation decisions regarding cryptographic algorithms, ledger choice, and selective disclosure methods.
- Compliance and audit procedures **MUST** explicitly validate adherence to this standard's decentralization, interoperability, and privacy requirements.