On Speech and Privacy

Jesse Katz & Eric Alston

Working draft, last edited September 30, 2026

This is independent research by Speech Without Borders, a 501(c)(3) nonprofit. It was not commissioned, compensated, or editorially supervised by any organization. The analysis is offered for the Ethereum Foundation's consideration, and feedback from the broader community of speech and privacy experts and stakeholders is welcome. Contact: speech.ngo/jesse

TLDR

Privacy is litigated as a prerequisite for speech and association in the United States, and that relationship can be useful in privacy advocacy outside the courtroom as well.

Privacy technology is infrastructure for expressive freedom.

Part I. Summary

The United States is the only G20 nation without a comprehensive national privacy law. Americans should be able to rely on the Fourth Amendment to protect them from unreasonable searches, but often cannot. For decades, data shared with any third party lost its protection. Courts have now rejected that rule for the ordinary use of phones and apps, yet the protections still stop short of information disclosed openly, and a public blockchain is open by design.

The gap persists because the government benefits from access to this information and private companies profit from collecting and selling it, including to the agencies that would otherwise need a warrant to obtain it. Alston and Cossar call this perverse alignment the institutional privacy dilemma, and it helps explain why federal privacy legislation keeps failing.

Our analysis focuses on areas where there are no trusted operators. People who build and run decentralized systems cannot arbitrarily change their rules or hand over user data they do not have, and attempting to regulate them as if they could would hold them responsible for systems they do not control.

Regulation by enforcement deters people from building and using legitimate privacy tools for lawful purposes. After Tornado Cash was sanctioned and its developers prosecuted, users and builders were observably less inclined to risk touching privacy tools.

The Ethereum Foundation has committed to privacy at the protocol level. Ethereum is general-purpose infrastructure that is public by default, so privacy has to be built in, as it should be in other technologies that support expressive activity.

While the Fourth Amendment still falls short of protecting this data, privacy has long been protected under the First Amendment's freedoms of speech and association. Without that privacy, exposure deters participation. Now activities like funding causes and participating in governance are happening on Ethereum, and they should be similarly protected, at the very least.

Open communication systems that allow people to freely speak, publish, and organize have earned constitutional protection of their own as general-purpose infrastructure that facilitates expressive activity. That protection did not depend on the proportion of expressive use. There are strong arguments for extending similar protection to Ethereum, but courts are still working out how existing rights translate to these new technologies.

On Ethereum, a single transaction can be a payment, a vote, and a signal of membership and identity, all at once. In funding rounds where contributions double as votes, one transfer moves the money, helps decide which projects are funded, and permanently marks what the sender supports. Disentangling protected expressive activity from ordinary traffic would require reviewing every transaction for its purpose, which is the surveillance the First Amendment guards against. This entanglement argument is the most ambitious here and not yet tested. The claim is not immunity. The standard proposed in Part II preserves the government's ability to pursue legitimate enforcement while barring the wholesale review that chills expression.

It is appropriate for privacy-focused projects to lead with privacy. Expression is only an additional tool, shaping how the ecosystem talks about, funds, develops, and organizes around privacy.

Protecting privacy through expressive rights can risk making privacy look merely instrumental, diminishing its value as an independent right. Where the Fourth Amendment falls short, this is the strongest protection US law presently offers, and the work of building privacy protections that stand on their own continues.

The structural relationship between speech and privacy should apply wherever privacy technologies support expressive activity. The AI tools people reason and draft with capture thinking in progress, and the dependence on privacy only deepens as augmented intelligence moves closer to the mind.

Part II develops these claims in detail, identifies the strongest objections, weighs the cost of grounding one right in another, and marks where the reasoning remains untested.

Part II. Analysis

Privacy has been defended through expression in the litigation over the sanctions on the privacy tool Tornado Cash and in the defense of Roman Storm, one of the developers, and the pattern has appeared outside blockchain. In 2016, the FBI sought to force Apple to write software disabling the San Bernardino iPhone's passcode protections, and Apple's response included a First Amendment claim that compelled code-writing

was compelled speech. Technology companies rallied behind Apple, and anti-encryption legislation failed in that political environment. No court ruled on the First Amendment claim, but the expression frame helped mobilize broader political and industry support for privacy infrastructure.

The First Amendment gives privacy on permissionless blockchain infrastructure its strongest available legal protection, with distinct jurisprudential leverage no other existing public-law route provides.

1. How Privacy Is Actually Defended

In its 2026 Mandate, the Ethereum Foundation (EF) names privacy as one of four non-negotiable core properties, alongside censorship resistance, open source, and security. These form an "indivisible whole" called CROPS, indispensable to Ethereum's development priorities. By the Mandate's account, privacy exists "to prevent structural power asymmetries from infringing on self-sovereignty and self-sovereign coordination," with users selectively negotiating their disclosures on top of "a base of freely available, unconditional privacy." That commitment is to a credibly neutral design, a non-discretionary, publicly verifiable rule that does not discriminate for or against specific people or outcomes (Buterin, 2020).

When the ecosystem's leading voices make the public case for privacy, they describe what it enables. Buterin's "Why I Support Privacy" (2025b) grounds its case in freedom, order, and progress. The EF's "Commitment to Privacy" frames it around democratic processes and "the freedom to think, communicate, and transact without surveillance." Privacy Stewards of Ethereum (PSE) describes privacy as giving people "the ability to organize, express, and transact freely."

In the Tornado Cash litigation, privacy was the central issue, but the constitutional argument for it rested on the First Amendment (*Coin Center v. Yellen*, N.D. Fla. 2023). Even critics skeptical of crypto's First Amendment claims have documented this structural dynamic (Langvardt, 2023). An earlier articulation of this relationship argued that blockchain activity involves protected expression and association (Wales and Ovelmen, 2019). The ecosystem's advocacy and its litigation arrive at the same structural relationship from two directions.

2. Privacy and Expression

Rights relate to each other structurally in specific contexts, and in some domains privacy operates independently of expression, while in others privacy interests may take precedence over expressive ones, as when privacy protections limit what can be published about identified individuals. For blockchain and Ethereum infrastructure in the United States, there are compelling reasons to treat the constitutional protections for expression and association as the strongest available legal basis for defending privacy.

In healthcare, intimate relationships, consumer finance, workplace surveillance, children's services, and biometric identification, the structural features of those contexts (fiduciary relationships, identified parties, power asymmetries, consent dynamics) favor privacy as the organizing value. Those features are largely absent or inverted in open blockchain infrastructure, where participation is permissionless, identity is pseudonymous, records are immutable, and exit is available by design. Expression and privacy can also directly conflict in some contexts (e.g., doxxing, public records, public figures). The alignment described here is a feature of this specific domain, not a universal condition.

Intellectual privacy, the protection of records of intellectual exploration, is essential to free speech (Richards, 2008, 2015). Privacy creates the breathing room in which individuals develop the capacity for independent thought and expression (Cohen, 2013). The premise that free expression depends on privacy is common ground, and this paper applies it to blockchain infrastructure and proposes intermediate scrutiny under *United States v. O'Brien* (1968), triggered by the inseparability of expressive and non-expressive activity on permissionless, public-by-default architecture.

The First Amendment protects not only individual expression but also the right of association, and the Supreme Court has recognized since *NAACP v. Alabama* (1958) that privacy in association can be essential to exercising that right. The Court has called speech, press, assembly, and petition "inseparable" since *Thomas v. Collins* (1945), which described them as "cognate rights" that cannot be isolated from one another for constitutional purposes.

These rights apply on blockchain networks like Ethereum as they do elsewhere. Expressive and non-expressive uses appear inseparable in practice. If that inseparability holds, protecting expression on this infrastructure may require protecting the infrastructure itself, extending the legal frame to activity that is not always expressive.

3. What Expression Requires

Privacy and expression exist in an asymmetric dependency, where expression requires the option of privacy but privacy serves purposes well beyond it.

Everything a person does on a public blockchain is permanently recorded and visible to anyone. A rider who pays a driver in crypto reveals the wallet they paid from, and the driver can then look up how much it holds and every transaction it has ever made. Having dropped the rider at home, the driver also knows where they live. Information like this can make a person a target for theft, extortion, or violence. Physical attacks on crypto holders reached record levels in 2025, roughly doubling the previous peak year (Lopp, 2026). Police in London found that attackers often knew what their victims held before they struck (TRM Labs, 2026). Guarding against harms like these is reason to protect privacy independent of expression.

The option to be private is particularly important for those whose views or associations make them vulnerable to retaliation, which is the concern that animated *NAACP v. Alabama* and the line of cases that followed it. Whistleblower protections reflect the same principle, since exposing institutional wrongdoing requires privacy the institution cannot revoke.

US law recognizes that certain relationships require zones of protected communication to function. The marital communications privilege protects spousal communications from compelled disclosure. The law accepts that spouses may keep secrets because the relationship's social value exceeds the evidentiary value of forcing disclosure. Compelling transparency does more than reveal information, since mandated openness changes the nature of the activity and what is revealed about it. The same logic applies to expression on transparent infrastructure, where people who know their activity is permanently visible behave differently from those who have the option of privacy.

For that option to be meaningful, privacy should generally be the default. Opt-in privacy is weaker because choosing it is a signal. On a transparent ledger, the act of seeking privacy can attract attention, which undermines the purpose.

This dependency concerns expression a person chooses to make, where the option to control one's visibility is what makes participation free rather than coerced. The distinction is especially significant in the on-chain context, where every action is permanently recorded and attributable. Interacting with the blockchain requires broadcasting a transaction to the network. To the extent any right is exercised via this infrastructure's features, it is carried out through a public act on-chain, so the dependency between expression and privacy follows from the architecture.

4. The Fourth Amendment Gap

Why protect privacy through expression at all? The Fourth Amendment protects against unreasonable searches and seizures. If digital privacy needs constitutional protection, why not use the amendment designed for it?

The Fourth Amendment, as currently interpreted, does not protect the records at issue here. The third-party doctrine, established in *United States v. Miller* (1976) and *Smith v. Maryland* (1979), holds that information voluntarily disclosed to a third party receives no Fourth Amendment protection. For decades, this swallowed nearly everything digital. Every search query is disclosed to a search engine, every exchange transaction to the exchange, each treated as though its owner had chosen to make it public.

Carpenter v. United States (2018) recognized that this framework breaks down for digital data, holding that historical cell-site location data is protected despite being held by a third party. In observing that comprehensive digital records expose intimate associations, *Carpenter* drew on Justice Sotomayor's concurrence in *United States v. Jones* (2012). She went further, warning that awareness of government monitoring "chills associational and expressive freedoms," which ties Fourth Amendment privacy to First Amendment expression. That connection has doctrinal roots predating *Carpenter*. In *Stanford v. Texas*(1965), the Court held that a warrant must describe the things to be seized with "the most scrupulous exactitude" when they are books seized for "the ideas which they contain," because no less a standard "could be faithful to First Amendment freedoms." *Carpenter* was cautious in scope and reserved whether its reasoning applied more broadly. *Chatrie v. United States* (2026) extended *Carpenter* to cell-phone location data held by Google, holding that a two-hour window and third-party storage do not defeat the Fourth Amendment.

The judiciary has moved to strengthen privacy for location data, but for blockchain, courts have not extended *Carpenter*. In *United States v. Gratkowski* (5th Cir. 2020), the court held that Bitcoin transaction records on a public blockchain receive no Fourth Amendment protection, reasoning that the data is publicly available and that users have no reasonable expectation of privacy in information they broadcast to a public ledger. That ruling governs the Fourth Amendment status of what users broadcast, and it does not address whether patterns of on-chain activity reveal expressive associations of the kind protected under *NAACP v. Alabama* and *Americans for Prosperity Foundation v. Bonta* (2021). *Carpenter*, and now *Chatrie*, recognized that aggregated data can reveal a qualitatively more intimate picture than isolated records, which is the premise the associational argument turns on. *Chatrie* also marks the boundary of Fourth Amendment protection, because its reasoning covered location data a user reasonably views as his own, not data broadcast to a public ledger, which is why protection for public on-chain activity is grounded in expression. In *Harper v. Werfel* (1st

Cir. 2024), the court held that cryptocurrency exchange records are not protected either, applying the bank-records rule *Chatrie* left undisturbed. The Supreme Court declined to review *Harper* in 2025, leaving the lower-court rulings in place.

The persistence of this gap is not doctrinal accident. It is the institutional privacy dilemma at work (Alston and Cossar, 2026). In the commercial data market, intelligence agencies acquire from brokers the data they would otherwise need warrants to compel, a practice the Office of the Director of National Intelligence confirmed in 2023 (ODNI, 2023). *Chatrie* narrowed compelled access to location data, yet it applied only to what the government may demand by warrant and left this commercial data market untouched. Enforcement against the broker industry proceeds case by case (*FTC v. Kochava, Inc.*, D. Idaho 2024). In the legislature, the American Privacy Rights Act of 2024 failed, as its predecessors had. The Fourth Amendment gap is a stable equilibrium in which the actors who could close it benefit from keeping it open.

The gap matters because people who know their activity is observable alter it accordingly, including by suppressing constitutionally protected expression and association.

Wikipedia page views for terrorism-related articles, none of them illegal to read, declined by just under 25 percent immediately following the Snowden revelations (Penney, 2016). The nothing-to-hide argument holds that people with nothing to hide have nothing to fear from surveillance. Stoycheff (2016) found the opposite. Most people aware of government surveillance are significantly less likely to express dissenting views, and the effect is strongest among those who considered such monitoring necessary and said they had nothing to hide. Searches for privacy-sensitive terms declined measurably after surveillance was revealed (Marthews and Tucker, 2017).

Chilling effects do not depend on state action, though government interference can make them far worse. On infrastructure where every transaction is permanently and publicly recorded, people who would otherwise engage in protected expression or association may avoid it entirely. Self-censorship is perhaps the most insidious form of suppression, since it requires no censor.

On blockchain infrastructure, the chilling mechanism also operates through prosecution. The indictment of Roman Storm charged three counts of conspiracy, to launder money, to operate an unlicensed money transmitting business, and to violate sanctions, and rested on the theory that Storm and two other cofounders developed, marketed, and operated Tornado Cash as a business run for profit. It alleged that Storm conducted, controlled, managed, and owned part of that business, that he knew a substantial portion of the funds it processed were criminal proceeds passed through it for concealment, and that the service received and handled funds of a sanctioned North Korean group. In *Dombrowski v. Pfister* (1965), the Supreme Court recognized that "[t]he chilling effect upon the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospects of its success or failure." The prosecution and the lingering uncertainty weigh on every developer considering whether to build privacy tools.

The resulting structural problem illustrates the institutional privacy dilemma at the enforcement level. On-chain transparency is the architectural default of a system designed for trustless verification, and the government did not impose it. Prosecuting developers who add privacy to transparent infrastructure ensures that this transparency remains a surveillance-enabling condition rather than a suboptimal design limitation that the community can address through engineering. The constitutional concern is that the government is punishing the people who make the tools that provide the privacy expression requires.

At the SEC Crypto Task Force Roundtable (December 15, 2025), SEC Chair Atkins warned that without privacy protections, crypto infrastructure could become "the most powerful financial surveillance architecture ever invented." Commissioner Peirce argued that privacy should be treated as "the norm, not an indicator of criminal intent." Commissioner Uyeda cited the Fourth Amendment directly, warning that indiscriminate aggregation of financial data creates opportunities for abuse. In an earlier speech criticizing Bank Secrecy Act surveillance, Peirce observed that "[t]he sledgehammer has become the tool of choice for monitoring for financial crimes." The President's Working Group report (July 2025) stated executive-branch support for "civil liberties protections surrounding privacy and the ability of individuals to privately transact on public blockchains." These concerns come from inside the government.

The Fourth Amendment asks whether the government conducted an unreasonable search. The First Amendment asks whether the government's actions suppress constitutionally protected expression and association. The First Amendment question stands whatever the answer to the Fourth, because the constitutional harm the former wards against is the suppression of protected activity, not the mechanics of observation.

5. Privacy as Constitutional Infrastructure

Promises not to surveil users are discretionary and can be revoked, coerced, or breached. Systems designed so they cannot surveil their users enforce privacy structurally. Digital constitutionalism names this practice, placing the protections beyond the discretion of whoever controls the system and beyond institutions whose incentives run toward eroding them (Alston, 2026).

Structural commitments matter even in systems where exit is cheap. Without them, every interaction requires assessing whether and how any information exposed might be exploited. Such commitments are what make participation rational. People and institutions need to be able to rely on these guarantees as load-bearing properties of the infrastructure. As networks scale, rising exit costs bind participants, and the commitments matter still more (Alston, 2025).

Ethereum is embedding these commitments at the protocol level. Censorship resistance ensures that participants and applications cannot be excluded. Enshrining privacy at the base layer is one of the five north-star objectives in the Strawmap (Drake et al., 2026). The Hardness protocol priority (March 2026) names privacy as a focus area through private transfers and anonymous broadcast. These commitments embody the principles of trustless design articulated in the Trustless Manifesto (Weiss, Buterin, and Posner, 2025).

The ecosystem's engineering orientation prioritizes protecting people without concentrating power, an approach called d/acc, or defensive acceleration (Buterin, 2023, 2025a). Privacy and compliance can be designed as complementary rather than mutually exclusive. Engineering and constitutional principles can productively reinforce one another. Architecture makes privacy durable in a way law alone cannot, and legal protection in turn would give those commitments the standing of a right.

6. The Constitutional Case for Privacy Through Expression and Association

If precedent supports treating privacy as a component of expression and association in this context, privacy would receive the constitutional protection that Fourth Amendment doctrine has not extended to this infrastructure. The arguments that follow are well-supported, but not yet established law. Future cases will define these margins, and we draw out here where we think they should fall to best ensure the protections contemplated by the First Amendment. The argument rests on three independent grounds, which are the *NAACP* associational privacy principle applied to specific on-chain activities, protection for general-purpose expressive infrastructure, and inseparability of on-chain categories. These range from the most well-established to the most ambitious. The *NAACP* principle is litigable under existing precedent, the infrastructure argument is developing as courts confront digital platforms, and inseparability is the broadest and least tested.

The Legal Baseline

The claim that "code is speech" rests on the *Bernstein* line of cases (originating in the Northern District of California in 1996 and affirmed by a Ninth Circuit panel before the case resolved without a final appellate ruling) and *Junger v. Daley* (6th Cir. 2000). There is no equivalent "code merits privacy" doctrine.

The three grounds are our arguments, and First Amendment claims about this technology have also been made more broadly, at three distinct levels of analysis. At the code level, the question is whether source code is protected expression. This is the domain of *Bernstein* and of Electronic Frontier Foundation and Coin Center advocacy. At the surveillance level, the question is whether dragnet surveillance of digital activity chills expression. This is the domain of *Carpenter*, the RCFP/Knight/FIRE amicus in *Chatrie*, and the SEC's own warnings about financial surveillance. At the infrastructure level, the question is whether expressive and non-expressive activity on permissionless, composable, public-by-default architecture can be separated without the surveillance that chills expression. Our analysis operates at the third level. Coin Center's missing-middleman paper develops the distinction between protected software publication and regulatable operation (Van Valkenburgh and Pieper, 2026), and the infrastructure-level argument here draws on that work. The three levels address different questions, not sequential ones. The infrastructure-level argument presupposes that monitoring on-chain activity can chill expression, which is a premise established in general by *NAACP v. Alabama* and its progeny but not yet tested judicially for public-by-default blockchain data specifically.

In *NAACP v. Alabama* (1958), the Supreme Court held unanimously that Alabama could not compel disclosure of the association's membership lists, observing that privacy in group association may be "indispensable to preservation of freedom of association." The lists were protected not because privacy is independently enumerated, but because forced disclosure would chill the exercise of associational and expressive rights. That principle has been extensively cited and extended well beyond its original civil rights context, including anonymous pamphlets (*Talley v. California*, 1960), anonymous campaign literature (*McIntyre v. Ohio*, 1995), and identification badge requirements (*Buckley v. ACLF*, 1999).

Applying the *NAACP* Principle On-Chain

The *NAACP v. Alabama* principle should extend to on-chain privacy. Expressive activity on permissionless blockchains requires privacy because the ledger records every action permanently.

"Expressive" spans a much broader class of activities than the merely political. Courts have extended protection to spending, association, anonymity, and symbolic conduct. Applied on-chain, expressive and

associational activity includes governance voting, Ethereum Name Service registration, NFT creation and collection, public goods funding, protocol signaling, and social protocol participation. These are the on-chain forms of voting in an association's elections, publishing under a chosen name, creating and collecting art, donating to causes, signing petitions, and joining clubs and forums.

In *NAACP v. Alabama*, the privacy interest was connected to a specific, identified expressive act (political association under documented threat). On-chain, the same infrastructure carries all of these activities simultaneously. The doctrine has not stayed confined to its founding facts. In *Bonta*, the Supreme Court applied the *NAACP* framework to a neutral charitable-registration regime that demanded donor information from the roughly sixty thousand charities renewing registration in California each year, none of which had been required to show any threat. A 6-3 majority held that the rule failed constitutional scrutiny because it was not narrowly tailored to the state's interest. The Court was explicit that a strong evidentiary showing of reprisal risk can be required of challengers where a regime is narrowly tailored to an important government interest, and is not required where the regime fails those criteria. The distance between a threatened civil rights organization and pseudonymous global infrastructure is real, but *Bonta*suggests the doctrine has already traveled most of it. What triggers the framework is the deterrent effect of compelled exposure on associational activity. The founding facts calibrate the required showing, not the doctrine's scope.

At minimum, the *NAACP* principle supports protecting these identifiable classes of on-chain expressive and associational activity under existing doctrine. It also supports the broader inference that where separating protected from unprotected transactions would require the surveillance the protection exists to prevent, the constitutional burden extends to the infrastructure that carries them. The Supreme Court has recognized, at least in plurality, that access to information is "a necessary predicate" to the meaningful exercise of speech rights (*Board of Education v. Pico*, 1982). Although the precedent is limited, the principle remains relevant.

The chilling mechanism from Section 4 is borne out by the response to the Tornado Cash sanctions. Use of Tornado Cash fell sharply (Wahrstätter et al., 2024). The retreat extended beyond the sanctioned tool, as other wallets withdrew from the US market, suspended mixing features, or geofenced American users, two of them within days of a later enforcement action against a related privacy wallet (Unchained, 2024). A similar concern surfaced inside government in a separate enforcement action. A sitting CFTC Commissioner dissented from the Ooki DAO case, warning that the Commission's approach "will have a chilling effect that discourages voting, thereby hindering good governance" (Mersinger, 2022).

The record of the response to the sanctions measures a sharp, ecosystem-wide retreat from privacy infrastructure. It does not separate the drop by activity type, so it cannot independently show governance, development, and financial use declining in lockstep. That inability to isolate which category was chilled does not by itself prove constitutional inseparability, but it is consistent with the inseparability argument's structural claim that enforcement aimed at one category of use suppresses all of them because the categories cannot be sorted at the infrastructure level without surveillance. The retreat is equally consistent with rational avoidance of legal risk, changing market conditions, or reputational caution, none of which requires the categories to be inseparable. A narrower reading remains possible, in which enforcement suppressed financial privacy rather than expression, returning the question to the Fourth Amendment ground Section 4 examined. The expressive and financial-privacy readings support the case for architectural privacy, though they differ on whether the constitutional basis is expressly First Amendment.

Removing privacy from this infrastructure would chill constitutionally significant expressive activity. That holds even if expressive use is a small share of what the network carries. The *NAACP* case did not hinge on whether a majority of members were politically active.

Privacy in governance also has doctrinal support, since *Bonta*'s protection did not turn on the political character of the association. The requirement fell for every charity subject to it, whatever its cause, and *NAACP* itself had treated the subject matter of association as immaterial, whether political, economic, religious, or cultural. DAO voting, governance token holdings, and delegation patterns are forms of associational activity. Whether courts extend the same protection to associational activity on-chain remains open, but the question concerns the medium, not the subject matter of the association.

Blockchain as General-Purpose Infrastructure

A broader argument extends protection to the infrastructure as a whole. Even if courts limit the *NAACP*principle to identified expressive activities, Ethereum merits robust protection as a general-purpose medium whose architecture is built to carry expressive and associational activity. Permissionlessness, immutable transparency, and the absence of trusted operators distinguish Ethereum from other programmable systems. Anyone can act, every action is recorded permanently and publicly, and no operator stands between a user and that exposure, so privacy exists on this infrastructure only where the architecture provides it. Nor is the range of what the medium carries fixed. Ethereum is Turing-complete, able to execute arbitrary logic rather than merely financial operations. Smart contracts support governance systems, identity systems, social protocols, publication systems, credential and trust systems, games, prediction markets, and programmable organizations alongside financial transactions. The dependency between expression and architectural privacy is what makes this infrastructure constitutionally distinctive.

The Supreme Court has addressed related questions for other digital infrastructure. *Reno v. ACLU* (1997) found "no basis for qualifying the level of First Amendment scrutiny" for the internet, unlike broadcast media. The Court did not ask what percentage of internet use was expressive. It looked at the medium's capacity for "relatively unlimited, low-cost" communication and its role as a place where any person "can become a town crier with a voice that resonates farther than it could from any soapbox." Twenty years later, in *Packingham v. North Carolina* (2017), the Court treated access to such a medium as itself a protected interest, striking a statute that barred registered sex offenders from social media. Two parts of that reasoning carry here. The Court cautioned that the internet's forces and directions are "so new, so protean, and so far reaching" that what courts say today might be obsolete tomorrow. It also declined to fix a young medium's constitutional status by the uses its critics emphasize, observing that inventions heralded as advances in human progress have long been exploited by the criminal mind, the railroad and the telephone among them. Neither case concerned financial or computational uses, and whether courts will extend the reasoning to infrastructure where those uses sit alongside expressive ones is untested. Still, the Court protected those media without weighing how much of their use was expressive, and we argue that the same should hold here.

This invites an obvious objection. Every payment rail, cloud service, and general-purpose network can facilitate expression, association, or publication by some users, and ordinary regulation of those systems does not thereby become presumptively unconstitutional. *NAACP v. Alabama* (1958), *Village of Schaumburg v. Citizens for a Better Environment* (1980), and *Reno v. ACLU* (1997) each protected a distinct relationship between expression and its supporting conditions, but none held that a multipurpose financial and computational infrastructure receives First Amendment protection merely because some of its uses are

expressive. The distinction is between architecture and discretion. A centralized exchange holding user funds can administer privacy through discretionary policy, and a regulator can direct it to. An immutable smart contract that no party can modify cannot be directed to do anything, and no single party controls the network it runs on. The payment rails and cloud services the objection names are of the first kind, and this infrastructure is of the second.

Inseparability

The most ambitious argument runs through inseparability and depends on the impossibility of sorting the expressive from the non-expressive without the surveillance that chills expression.

A social protocol relies on an identity system, which relies on financial primitives, which connect to governance tools, so the layers are inextricable. Permissionlessness means anyone can deploy any application, and composability means those applications interact by design. Together, these properties leave the range of on-chain activity undefined and undefinable at the infrastructure level, because anyone can deploy new kinds of applications faster than any fixed taxonomy can catalog them.

Funding a DAO is an associational act, donating to a public goods funding round is expressive and sometimes political, and purchasing governance tokens acquires the capacity to participate in organizational decision-making. Each is a single act, and none is purely financial, any more than a campaign contribution is purely financial. Under *Buckley v. Valeo* (1976), spending money to facilitate political expression is protected by the First Amendment. *Village of Schaumburg v. Citizens for a Better Environment* (1980) established the same protection for charitable solicitation, holding that solicitation is "characteristically intertwined with informative and perhaps persuasive speech" and protected even when the expression is not political. If the *Schaumburg* principle applies, the financial character of many blockchain transactions does not remove them from First Amendment concern when they are inextricable from expressive activity.

This inseparability claim is about constitutional categorization, whether an activity counts as expression, not about regulatory compliance. Regulators already sort transactions to determine whether funds touch sanctioned sources, which tracing fund flows can answer without inquiry into the transactor's purpose. Constitutional categorization is different from that sorting, because it asks whether a transaction is expressive, and that cannot be answered by tracing flows. A governance vote is likely classifiable as associational activity, and a token transfer between a user's own wallets as non-expressive financial activity, but a token purchase that simultaneously acquires governance rights, represents a financial investment, and signals community membership cannot be classified by expressive character without evaluating the transactor's purpose and context, which is the kind of inquiry the First Amendment restricts.

Commercial chain-analysis firms classify on-chain activity every day by transaction type and risk, but they sort by observable characteristics like contract interaction, token type, and fund flow, not by communicative purpose. Classifying by communicative purpose requires an inquiry deep enough to constitute the surveillance the constitutional protection exists to prevent. Compliance tools that verify whether funds originate from sanctioned sources, without categorizing whether a transaction is expressive, financial, or associational, illustrate the line. The International Emergency Economic Powers Act, the statute under which Treasury sanctioned Tornado Cash, gives the President no authority to regulate or prohibit any "postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value," or the import and export of information "whether commercial or otherwise." These provisions are

cited as a point of reference and not for any protection they might extend to activity on a public blockchain. The distinction between sorting and categorization is cleaner in principle than in practice, and a court could conclude that the same analytical tools serve both purposes. We think they are functionally different operations, and collapsing them would turn compliance itself into the purpose inquiry the First Amendment restricts.

In *Schaumburg*, the Court recognized that canvassers soliciting for charity were "necessarily more than solicitors for money." The financial activity was itself expressive, and that is both what *Schaumburg*uniquely supplies and the limit of what it supplies. The obvious answer available to a government is that the canvasser was speaking while the transactor is not, so that a restriction attached to non-expressive conduct never meets the doctrine at all. The associational ground does not depend on winning that exchange. *NAACP* protected association as such, silent membership rather than any act of speaking, so its protection attaches without asking whether the underlying act was expressive, and *Bonta* applied the same framework to donor records, which are financial documents through and through. For on-chain activity that is itself expressive, *Schaumburg* and *Buckley v. Valeo* apply directly. For the associational character of funding, holding, and voting, *NAACP* and *Bonta* carry the weight, and they are the stronger anchors because they offer no expressive-act handle to grasp. The frontier question is whether these principles extend to infrastructure where expressive and non-expressive activity are inextricable rather than intertwined within a single act.

The argument does not rest on classifying each transaction as expressive. Its strength is independent of how much on-chain activity is expressive, which cannot be measured without the surveillance at issue. Protecting expressive uses through as-applied challenges would not avoid that surveillance, since each challenger would have to show the government what a transaction expressed or which association it served. Ordinary payments between wallets are one activity this analysis does not cover. To what extent activity can be sorted is a margin courts will inevitably probe.

Carpenter supports this reasoning from a different direction. The Court recognized that digital data can be qualitatively different from analog records, and that pervasive digital surveillance creates constitutional concerns that mechanical application of older doctrines does not address. Describing a retained record of everyone's movements, the Court wrote that "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." The qualitative difference matters even more for the First Amendment analysis, because the severity of the chilling effect is a direct function of how pervasive, revealing, and inescapable the surveillance is. Digital surveillance on transparent infrastructure is all three.

Critics can object that the ecosystem chose to build infrastructure that prevents categorization and now asks courts to constitutionalize that choice, but the objection would be imprecise. The ecosystem is designed for trustless verification through transparency, and privacy remedies the resulting exposure. Permissionlessness and composability were deliberate choices, while public-by-default transparency was the price of trustless verification with the cryptography available at the time, a constraint rather than a goal (Nakamoto, 2010). The entanglement is a necessary consequence of that architecture, and builders in the ecosystem did not separately engineer it to prevent categorization.

If these arguments hold, the strongest constitutional case for privacy on this infrastructure is that expression, which the Constitution already protects, cannot function here without it.

Regardless of how courts resolve the inseparability and infrastructure questions, narrower conclusions follow independently. On-chain governance voting, delegation, token-based association, and related signaling

practices implicate associational privacy under *NAACP v. Alabama* (1958) and *Americans for Prosperity Foundation v. Bonta* (2021). Privacy-enhancing design would also remain constitutionally relevant to chilling analysis where the practical alternative is exposure that predictably deters participation.

7. The Contested Landscape

The ecosystem's litigation pattern, which uses the First Amendment for developers' code and the Fourth Amendment for users' privacy, illustrates a structural tension. The Coin Center amicus in the Roman Storm case (April 2024) shows that even when the explicit strategy is to argue the two tracks separately, privacy still appears as the content of protected speech, nested within the expression frame. If expressive and non-expressive uses of the infrastructure cannot be separated, the doctrinal division between the First and Fourth Amendments may not reflect the underlying architecture. Whether users' on-chain privacy can receive First Amendment protection directly, through the *NAACP* principle, rather than requiring a separate Fourth Amendment track, is a question Coin Center put to a court in its own challenge to the sanctions, and one this analysis raises but cannot resolve.

In *Chatrie*, the Supreme Court held that acquiring a person's cell-phone location data through a geofence warrant is a Fourth Amendment search, extending *Carpenter* and rejecting the argument that a short window or third-party storage removes the data from the Amendment's protection. An amicus brief urged the Court to treat privacy as a precondition for expression and to apply the Fourth Amendment with the "scrupulous exactitude" that *Stanford v. Texas* requires (Reporters Committee for Freedom of the Press et al., 2026). Drawing on the Court's own vocabulary, the brief invoked the "cognate rights" of *Thomas v. Collins* and the "vital relationship" between privacy and First Amendment freedoms, and it argued that geofence warrants chill expression by "ensnaring everyone to develop the individualized suspicion" that should precede a search. The Court resolved the Fourth Amendment question in a privacy-protective direction without adopting that First Amendment theory, so it remains available and untested.

By the Court's own account, a two-hour window of location data is enough for officers "to target one-off events of potential interest," such as "a gun show, say, or a political rally." A public blockchain, by contrast, keeps a permanent public record of all on-chain activity. We argue that such a record burdens expression and association whether or not anyone ever reads it.

Where courts have ruled on the expression argument directly, it has lost. In the Storm case, Judge Failla rejected the First Amendment defense, drawing a distinction between code's expressive function (potentially protected) and its "functional capability" (not protected). She held that intermediate scrutiny would be satisfied because the government has a "substantial interest in promoting a secure financial system." Coin Center argues the distinction rests on outdated case law (Van Valkenburgh, 2024), and the post-trial motion for acquittal challenges it directly. Storm was convicted on one count (conspiracy to operate an unlicensed money transmitting business), but the jury deadlocked on both more serious charges (money laundering conspiracy and sanctions conspiracy). The acquittal motion and a retrial on the deadlocked counts, now set for 2027, leave the legal questions unresolved. Judge Failla's ruling addresses the code level, asking whether source code's functional capability is protected expression. The infrastructure-level question asks instead whether expressive and non-expressive activity can be separated on the infrastructure without the surveillance that chills expression. Whether Judge Failla's expression and functional-capability distinction can withstand *Schaumburg*'s reasoning that intertwined categories cannot be separated remains open.

The inseparability argument still bears on Judge Failla's reasoning. If expressive and functional dimensions of on-chain activity cannot be separated without surveillance, then the distinction may infringe the very rights it purports to protect. The distinction also conflicts with the logic of *Reno* and *Packingham*, which protects access to and use of a medium, not just the medium's publication function.

First Amendment arguments have historically been used not only to defend expression but to block regulation, including privacy regulation (Richards, 2005). The risk that expression claims become a tool for regulatory avoidance rather than rights protection is real. The argument uses expression to defend privacy, not to block it, and proposes intermediate scrutiny under *O'Brien* rather than categorical protection, which preserves the government's ability to pursue legitimate enforcement objectives. Privacy at the protocol layer applies to every user and every transaction, expressive or commercial, by the same architectural property, which is the credible neutrality defined earlier. Privacy infrastructure of this kind cannot be opportunistically deployed to shield commercial interests from legitimate regulation while exposing others, because the architecture has no mechanism for the selectivity that opportunism requires.

In *Van Loon v. Department of the Treasury* (5th Cir. 2024), the court held that immutable smart contracts are not sanctionable "property" under IEEPA, and Treasury subsequently delisted Tornado Cash in March 2025. Earlier, both district courts to hear users' challenges to the designation had rejected their First Amendment claims. In *Van Loon*, the district court did so at the threshold, holding that the designation barred only transactions while leaving analysis and teaching of the code untouched, and faulting the summary judgment record without engaging First Amendment doctrine. In Coin Center's suit, brought with users who donated through the tool, the court held that the designation did not implicate the First Amendment because, unlike *Bonta*, it compelled no association to disclose its donors or members and left other ways to give privately (*Coin Center v. Yellen*, N.D. Fla. 2023). No appellate court reviewed either First Amendment ruling, since the *Van Loon* plaintiffs did not appeal that loss and the Eleventh Circuit vacated the Florida judgment on the parties' joint motion after the delisting, which leaves the questions this analysis raises open. The Fifth Circuit treated immutable smart contracts as tools rather than services, which is consistent with the infrastructure-level framing. Neither smart contracts nor the protocol layer in its entirety is subject to the discretionary control of any legally identifiable actor once immutably deployed (Alston, 2026).

The speech-integral-to-criminal-conduct exception (*Giboney v. Empire Storage*, 1949) would apply if courts classify privacy infrastructure as "integral to" money laundering. Infrastructure that no operator controls, applying to every use by the same mechanism, is not integral to the crimes conducted through it, any more than the internet is integral to fraud conducted online or the postal system is integral to mail fraud. How *Giboney* applies to infrastructure, as distinct from the acts conducted through it, has not been settled in this context.

The proportionality question is open under *O'Brien*, which would likely govern content-neutral infrastructure regulations. A court could conclude that the government is regulating functionality rather than message, and that intermediate scrutiny is satisfied if the means burden expression no more than is essential to the interest, a standard that does not require the least restrictive means available (*Ward v. Rock Against Racism*, 1989). In *Cohen v. Cowles Media* (1991) the Court held that a law of general application binds the press like everyone else, and in the same opinion marked where the rule stops, making clear that a state may not define by content which expression triggers liability. The government would invoke the rule here, and the statutes as written let it, attaching liability to control over funds, knowledge about particular funds, and dealings with designated persons, with nothing keyed to what a transaction expresses. The rule applies only as far as those triggers and fails wherever a charge comes to rest on what the activity expressed. A neutral statute enforced

only against expressive uses meets a different objection, selective prosecution, which is available in principle and hard to prove. Both exits depend on how a case is brought.

The rule excuses only an incidental burden, and the enforcement itself shows this one is not. The government's interest in preventing money laundering is substantial. In its 2023 proposal to designate foreign mixing transactions a primary money laundering concern, the Financial Crimes Enforcement Network (FinCEN) recorded that North Korea's Lazarus Group laundered proceeds of a theft of nearly $620 million through mixers to finance the country's weapons programs, that the ten most common ransomware strains in its own filings sent approximately $35.2 million to mixers in the first half of 2021, and that non-state hackers moved the proceeds of large-scale theft the same way. The same document bounds the harm. FinCEN traced 13 percent of deposits at the ten largest mixers to known illicit activity and a third to high-risk sources, and even with its warning that the true share was probably higher, most deposits had no identified connection to either.

The enforcement record suggests the means swept far past that interest. The sanctions on Tornado Cash and the prosecutions of privacy developers were followed by a sharp, ecosystem-wide reduction in the use of the privacy infrastructure on which constitutionally protected activity depends, extending well beyond the illicit conduct enforcement targeted. That overreach is not just a feature of how this enforcement happened to unfold. Enforcement here has two forms. Aimed at the illicit conduct alone, it traces the proceeds. Aimed at the tool, as it was, it falls on every use, the protected ones included. FinCEN faced the same choice in the same proposal. It considered confining the rule to North Korean and terrorist actors and rejected the idea, since institutions "would typically have insufficient information to determine" whether a transaction was North Korean, a limit "true of any similarly narrow approach, regardless of the actors involved," and since a narrower rule would discard reports "of equal or greater value." Its rule would instead have institutions "presume" every mixing transaction to be of primary money laundering concern, which answers the sorting problem by reporting every user instead of sorting any. A burden placed on every use is built into the means, not incidental to them.

Targeted enforcement through chain analysis is available and has already produced successful prosecutions. Cryptographic compliance tools can pursue the same enforcement objectives without requiring the state to sort transactions by expressive character. Those tools show the same interest can be met with far less burden on expression, and they let compliance proceed without converting constitutional analysis into surveillance. Whether courts would accept that characterization is open, and deployment of the tools at scale remains in progress. The availability of targeted enforcement and cryptographic compliance presents a colorable argument about alternative means that could make it harder for the government to prevail under intermediate scrutiny.

The institutional privacy dilemma produces contradictory outputs on blockchain specifically. Treasury's own mixer report (March 2026) acknowledged that mixers have lawful privacy uses. The DOJ's Blanche memo (April 2025) instructed prosecutors not to target tools for end users' conduct. A senior DOJ official stated publicly that "writing code without ill intent is not a crime" (August 2025). The DOJ's Southern District of New York sought a retrial of Roman Storm for operating a mixer. The government simultaneously endorses privacy in principle and prosecutes privacy developers in practice. Official pressure that drives books out of circulation is a "system of informal censorship" and violates the Constitution even when no one is prosecuted, the Supreme Court held in *Bantam Books v. Sullivan*(1963). There, a state commission's notices listing titles it considered objectionable for sale to minors had led a distributor to stop carrying them, since people "do not lightly disregard public officers' thinly veiled threats." By the government's statements, the tools have lawful

uses and writing their code without ill intent is not a crime, so for every developer who was not charged, the prosecutions are that threat without the veil, and the withdrawal of privacy services that followed is the harm *Bantam* condemns, not a side effect of enforcement.

The Communications Assistance for Law Enforcement Act (CALEA) is instructive as a matter of policy, if not doctrine. Congress mandated surveillance capabilities in telecom networks, yet also prohibited requiring "any specific design of equipment, facilities, services, features, or system configurations." The mandated backdoors were later exploited in the Salt Typhoon breach (2024), after which US cyber agencies publicly recommended end-to-end encrypted communications (CISA, 2024). The government recommending end-to-end encryption has prosecuted the people who build privacy tools on blockchain networks. The contradiction does not resolve the legal questions, but it does illustrate the practical risks of mandated surveillance infrastructure, which bear on proportionality.

The ecosystem's response to these pressures inverts the "design choice" objection. Privacy is a non-negotiable core property, necessary for the platform to fulfill its purpose, not an attempt to evade regulation. The compliance toolkit reflects this in zero-knowledge proofs with association set providers for jurisdictional compliance (Buterin et al., 2024), automatic proofs that tokens are not from sanctioned sources, and wallet infrastructure that integrates privacy with optional public linkage for institutional audits.

If expression on this infrastructure receives First Amendment protection because expressive and non-expressive uses cannot be separated, what prevents the same logic from extending to every general-purpose network? The limit turns on whether any party holds discretion over what moves across the network, the same architecture-versus-discretion distinction drawn above. Compliance continues in a different form, attached to whoever holds that discretion. Where no operator with discretion exists, the absent intermediary cannot be invented by burdening developers, software publishers, interface maintainers, or node operators with surveillance-equivalent compliance obligations. Whether a particular system lacks such an operator is a factual inquiry, and in blockchain networks like Ethereum the absence is architectural.

The principle has a working counterpart in Section 230 of the Communications Decency Act, under which an online service is not treated as the publisher of what its users post and can carry it without reviewing every message. Developers, software publishers, interface maintainers, and node operators occupy a comparable position toward the activity that runs on the infrastructure they build and maintain, and the limiting principle applies the same logic to them, since a duty to review everything on the network would be similarly unreasonable. Congress enacted Section 230 in 1996, the year after a New York court ruled in *Stratton Oakmont v. Prodigy* (1995) that an online service could be held responsible for what its users posted because it had moderated some of it. Partial moderation had produced a duty to review everything, and the statute removed that duty from a service that had the ability and made the effort. Where the architecture leaves no comparable choice to make, the case is stronger still.

The constitutional objection to a duty of that kind is older than the internet. In *Smith v. California* (1959) the Court reversed the conviction of a Los Angeles bookseller under an ordinance that made him criminally liable for an obscene book on his shelves whether or not he knew what it contained. The Court reasoned that liability without knowledge would force him to inspect everything he stocked and to sell only what he had read, and that a bookseller so confined restricts the public's access to books the ordinance did not cover. The demand came so close to requiring omniscience that the Court held it unreasonable.

The comparison borrows reasoning from both sources and a holding from neither. Section 230 is a statute, and nothing in this argument turns on whether the Constitution would have required it. *Smith*held only that the ordinance could not punish a bookseller for a book he knew nothing about, and the expressive character of the books was never in question. The expressive character of activity on this infrastructure is what the government disputes.

The layers those parties occupy have already been tried as substitutes for the absent intermediary. When Treasury sanctioned Tornado Cash in August 2022, its website and code repositories were taken down, the node operators that served its interface cut it off (The Block, 2022), a stablecoin issuer froze the tokens it had issued that were held in the mixer's pool, and from the next month the four largest block builders, services that assemble transactions into Ethereum's blocks, censored transactions that touched the listed addresses (Wahrstätter et al., 2024), though the listing named none of these companies. Each controlled its own service and nothing beyond it, so the contracts continued to function despite the efforts to shut them down, the freeze only stopped one token and left the ether pools running, and the transactions some builders censored were eventually included by others. The listing also named the contract addresses, and the Fifth Circuit observed that those immutable contracts kept operating in spite of the designation. Use of the tool fell sharply and access to it narrowed, but neither stopped entirely, and the court found that the North Korean actors the listing targeted were not blocked from retrieving their stolen assets. None of these layers can single out unlawful use. They did nothing but add cost and delay for all users, and since a mixer's privacy comes from the number of users in it, that pressure fell on lawful use first and weakened the tool for the unlawful user only by driving the legitimate ones out.

Enforcement law applies to parties through the funds they hold, the businesses they run, the criminal proceeds they knowingly move, or the sanctions imposed on them. FinCEN, in its 2019 guidance, treats a wallet provider as a money transmitter when it holds "total independent control over the value," which is the discretion a centralized exchange exercises over the user funds it holds. For mixers it separates a service that takes custody of users' funds, which is a money transmitter, from a supplier of anonymizing software, which is not. Every custodial service, whether wallet, exchange, or mixer, must register, identify its customers, keep and report records, and respond to lawful process. Criminal liability for unlicensed money transmitting falls on whoever conducts, controls, manages, supervises, directs, or owns such a business, including a business that transmits funds its operator knows to be the proceeds of crime. Sanctions attach to designated persons. None of that requires sorting the network's activity by what it expresses.

The same law applies to developers who retain control of what they deploy. FinCEN treats a developer who "uses or deploys" an application to transmit money as a money transmitter, and Treasury can designate anyone who provides technological support to sanctioned activity. The district court in Storm declined to treat the case as a prosecution for writing code, since the business charged extended beyond the immutable pool to the interface the founders controlled and the relayers who collected fees. The court's further holding, that control of the funds is not an element of the statute, has not been tested on appeal. What enforcement may not do is invent the absent intermediary by burdening parties who lack control, or sort the network's activity by its expressive character. No layer of the network can single out unlawful use, so any burden placed on the network to suppress unlawful activity suppresses lawful activity with it. In *Ashcroft v. Free Speech Coalition* (2002) the Court held that the government "may not suppress lawful speech as the means to suppress unlawful speech," and *Packingham* applied that rule under intermediate scrutiny.

8. Conclusion

We began with the observation that the Ethereum ecosystem already defends privacy through expression in court and, in its public advocacy, describes privacy by what it enables. We identified the structural relationship on which the litigation and the advocacy converge and developed its constitutional implications. The finding strengthens the constitutional case for privacy.

The constitutional case has three independent grounds. First, existing precedent supports extending the *NAACP* associational privacy principle to specific on-chain activities including governance, delegation, and public goods funding. Next, Ethereum merits protection as general-purpose expressive infrastructure, on reasoning the Court has applied to the internet but has not yet extended this far. Finally, and most ambitiously, expressive and non-expressive on-chain activity cannot be separated without the surveillance that chills expression. *Chatrie v. United States* (2026) moved Fourth Amendment doctrine for cell-phone location data, but records on a public ledger or at an exchange remain outside its protection. That gap is stable, since the actors who could close it benefit from keeping it open, and the legislative path has failed repeatedly at institutional fault lines. The government did not create the architectural transparency of public blockchains, but by prosecuting developers who build privacy into that infrastructure, it is preventing the remedy.

These claims are untested at the appellate level, and the doctrinal questions are open. The relationship between expression and privacy is already in litigation, and we articulate it for the work of building, funding, and advocacy that depends on the same constitutional foundation.

The necessity of protecting privacy through expression makes the case for developing protections that do not depend on it. Whether courts will extend the inseparability principle to blockchain infrastructure, and whether the limiting principle proposed here holds under adversarial scrutiny, are questions for judges, legal scholars, and the domain experts best positioned to evaluate them.

In the meantime, the ecosystem is building technologies that give people the option to exercise rights they already have, within rules that already exist.

This relationship likely holds beyond Ethereum, and Appendix A develops that extension toward privacy of thought and augmented intelligence.

References

Cases

- *Americans for Prosperity Foundation v. Bonta*, 594 U.S. 595 (2021)
- *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)
- *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963)
- *Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999), opinion withdrawn pending rehearing en banc, 192 F.3d 1308 (9th Cir. 1999)
- *Board of Education v. Pico*, 457 U.S. 853 (1982)
- *Buckley v. American Constitutional Law Foundation, Inc.*, 525 U.S. 182 (1999)

- *Buckley v. Valeo*, 424 U.S. 1 (1976)
- *Carpenter v. United States*, 585 U.S. 296 (2018)
- *Chatrie v. United States*, No. 25-112, 609 U.S. ___ (2026)
- *Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991)
- *Coin Center v. Yellen*, No. 3:22-cv-20375, 2023 WL 7121095 (N.D. Fla. Oct. 30, 2023), vacated, No. 23-13698 (11th Cir. July 3, 2025)
- *Dombrowski v. Pfister*, 380 U.S. 479 (1965)
- *Federal Trade Commission v. Kochava, Inc.*, No. 2:22-cv-00377-BLW, 2024 WL 449363 (D. Idaho Feb. 3, 2024)
- *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490 (1949)
- *Harper v. Werfel*, 118 F.4th 100 (1st Cir. 2024), cert. denied, No. 24-922 (U.S. June 30, 2025)
- *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000)
- *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995)
- *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974)
- *NAACP v. Alabama*, 357 U.S. 449 (1958)
- *Packingham v. North Carolina*, 582 U.S. 98 (2017)
- *Reno v. ACLU*, 521 U.S. 844 (1997)
- *Smith v. California*, 361 U.S. 147 (1959)
- *Smith v. Maryland*, 442 U.S. 735 (1979)
- *Stanford v. Texas*, 379 U.S. 476 (1965)
- *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)
- *Talley v. California*, 362 U.S. 60 (1960)
- *Thomas v. Collins*, 323 U.S. 516 (1945)
- *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020)
- *United States v. Jones*, 565 U.S. 400 (2012)
- *United States v. Miller*, 425 U.S. 435 (1976)
- *United States v. O'Brien*, 391 U.S. 367 (1968)
- *United States v. Storm*, No. 1:23-cr-00430 (S.D.N.Y.)
- *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024)
- *Village of Schaumburg v. Citizens for a Better Environment*, 444 U.S. 620 (1980)
- *Ward v. Rock Against Racism*, 491 U.S. 781 (1989)

Academic and Policy Sources

- Alston, Eric. "The Persistent Centralization of Corporate Governance: An Organizational Coase Theorem." SSRN 4039320 (2025).
- Alston, Eric. "Digital Constitutionalism: Constraining Authority in Network-Coordinated Digital Orders." SSRN 6417218 (2026).
- Alston, Eric, and Sofia Cossar. "The Institutional Privacy Dilemma: Technological Change and the Coevolution of Privacy Institutions." SSRN 4847953 (2026).
- Buterin, Vitalik. "Credible Neutrality As A Guiding Principle." nakamoto.com (January 3, 2020).
- Buterin, Vitalik. "My Techno-Optimism." vitalik.eth.limo (November 27, 2023).
- Buterin, Vitalik. "d/acc: One Year Later." vitalik.eth.limo (January 5, 2025a).
- Buterin, Vitalik. "Why I Support Privacy." vitalik.eth.limo (April 14, 2025b).
- Buterin, Vitalik, et al. "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium" (Privacy Pools). Blockchain: Research and Applications 5, 100176 (2024).

- Cohen, Julie E. “What Privacy Is For.” Harvard Law Review 126(7), 1904-1933 (2013).
- Coin Center. Amicus Curiae Brief in *United States v. Storm*, No. 1:23-cr-00430 (S.D.N.Y. Apr. 5, 2024).
- Cybersecurity and Infrastructure Security Agency (CISA). Mobile Communications Best Practice Guidance (December 18, 2024).
- Drake, Justin, et al. “L1 Strawmap.” strawmap.org (2026).
- Langvardt, Kyle. “Crypto’s First Amendment Hustle.” Yale Journal of Law & Technology 26, 130 (2023).
- Lopp, Jameson. “Known Physical Bitcoin Attacks.” github.com/jlopp/physical-bitcoin-attacks (accessed September 29, 2026).
- Marthews, Alex, and Catherine Tucker. “Government Surveillance and Internet Search Behavior.” SSRN 2412564 (2017).
- Mersinger, Summer K. “Dissenting Statement of Commissioner Summer K. Mersinger Regarding Enforcement Actions Against: 1) bZeroX, LLC, Tom Bean, and Kyle Kistner; and 2) Ooki DAO.” Commodity Futures Trading Commission (September 22, 2022).
- Nakamoto, Satoshi. “Re: Not a suggestion.” bitcointalk.org (August 11, 2010).
- Office of the Director of National Intelligence. Senior Advisory Group Panel on Commercially Available Information (declassified report, dated January 2022, released June 2023).
- Peirce, Hester M. “Peanut Butter & Watermelon: Financial Privacy in the Digital Age.” Speech at the Science of Blockchain Conference (August 4, 2025).
- Penney, Jonathon W. “Chilling Effects: Online Surveillance and Wikipedia Use.” Berkeley Technology Law Journal 31(1), 117 (2016).
- President’s Working Group on Digital Asset Markets. “Strengthening American Leadership in Digital Financial Technology.” (July 2025).
- Reporters Committee for Freedom of the Press, Knight First Amendment Institute at Columbia University, and Foundation for Individual Rights and Expression. Amicus Curiae Brief in *Chatrie v. United States*, No. 25-112 (U.S. Mar. 2, 2026).
- Richards, Neil M. “Reconciling Data Privacy and the First Amendment.” UCLA Law Review 52, 1149 (2005).
- Richards, Neil M. “Intellectual Privacy.” Texas Law Review 87, 387 (2008).
- Richards, Neil M. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press (2015).
- Stoycheff, Elizabeth. “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring.” Journalism & Mass Communication Quarterly 93(2), 296-311 (2016).
- TRM Labs. Wrench Attacks: Crypto-Enabled Violent Targeting. White paper, with the Metropolitan Police Service (July 30, 2026).
- United States Department of Justice. Ending Regulation By Prosecution. Memorandum from Deputy Attorney General Todd Blanche (April 7, 2025).
- United States Department of the Treasury. Tornado Cash Delisting. Press release (March 21, 2025).
- United States Department of the Treasury. Innovative Technologies to Counter Illicit Finance Involving Digital Assets (March 2026).
- United States Department of the Treasury, Financial Crimes Enforcement Network. Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies. FIN-2019-G001 (May 9, 2019).
- United States Department of the Treasury, Financial Crimes Enforcement Network. Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern. 88 Fed. Reg. 72701 (October 23, 2023).

- United States Department of the Treasury, Office of Foreign Assets Control. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Press release (August 8, 2022).
- Van Valkenburgh, Peter. "Analysis: The disappointing denial of Tornado dev's motion to dismiss." Coin Center (October 8, 2024).
- Van Valkenburgh, Peter, and Lizandro Pieper. "Software is Speech: Why Regulators Cannot Invent the Missing Middlemen." Coin Center (April 2026).
- Wahrstätter, Anton, et al. "Blockchain Censorship." Proceedings of the ACM Web Conference 2024 (WWW 2024), 1632-1643.
- Wales, Justin, and Richard J. Ovelmen. "Bitcoin is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment." University of Miami Law Review 74(1), 204 (2019).
- Weiss, Yoav, Vitalik Buterin, and Marissa Posner. "The Trustless Manifesto." trustlessness.eth.limo (November 11, 2025).

Ecosystem Sources

- SEC Crypto Task Force Roundtable (December 15, 2025): https://www.sec.gov/newsroom/meetings-events/crypto-task-force-roundtable-financial-surveillance-privacy
- Ethereum Foundation Mandate (2026): https://blog.ethereum.org/2026/03/13/ef-mandate
- Ethereum Foundation, "A Deeper Look at a New Protocol Cluster Priority: Hardness" (March 18, 2026): https://x.com/ethereum/status/2034307029272293478
- Ethereum Foundation Commitment to Privacy (October 8, 2025): https://blog.ethereum.org/2025/10/08/privacy-commitment
- Privacy Stewards of Ethereum mission (2025): https://pse.dev/about
- Apple-FBI encryption dispute (2016): https://epic.org/documents/apple-v-fbi-2/
- The Block, "Infura and Alchemy are now blocking access to Tornado Cash" (August 9, 2022): https://www.theblock.co/post/162402/infura-and-alchemy-blocking-access-to-tornado-cash
- The Block, "'Writing code without ill intent is not a crime,' says US DOJ official following Tornado Cash verdict" (August 21, 2025): https://www.theblock.co/post/367858/writing-code-without-ill-intent-is-not-a-crime-says-us-doj-official-following-tornado-cash-verdict
- Unchained, "zkSNACKs Blocks US Users From Wasabi Wallet" (April 29, 2024): https://unchainedcrypto.com/zksnacks-blocks-us-users-from-wasabi-wallet/

Appendix A. Privacy of Thought & Augmented Intelligence (early research)

Contact: speech.ngo/jesse

The ideas in this appendix are exploratory and are included to invite feedback. We are researching these connections and welcome collaboration with people who have deeper expertise in these domains.

The relationship between privacy and expression is not unique to Ethereum. If it is visible where activity is mixed, financial, and less obviously expressive, it should become easier to see in technologies closer to communication, deliberation, and cognition that depend on the same privacy primitives.

When a person uses an AI assistant to reason through a problem, explore a sensitive question, or draft an argument, the interaction captures cognition in progress, not completed behavior. This is qualitatively different from the phone data *Carpenter* and *Chatrie* addressed because it is participatory. The person and the tool co-produce the output, so the data is fused with the thinking itself. One analysis argues that AI-generated speech is protected by the First Amendment, both through the rights of programs' creators and through the rights of users to create their own speech using AI tools (Volokh, Lemley, and Henderson, 2023). Others have argued that extending speech protection to AI output misapplies existing doctrine (Salib, 2024). If the first analysis is correct, the user's iterative engagement with an AI tool is the process through which expression is formed, which is analogous to the editorial judgment that courts have recognized as part of the expressive process (*Miami Herald Publishing Co. v. Tornillo*, 1974). Surveillance of that process chills expression by a mechanism like the one documented for on-chain activity. That step is our reasoning, not theirs, and it is untested.

In December 2025, eight browser extensions with more than eight million users between them were found to have been silently harvesting AI conversations from the major chatbot platforms for sale to a data broker (Koi Security, 2025). Privacy that runs through intermediaries depends on the integrity of every link between the user and the service, and any compromised link exposes the data. Architectural privacy, where no trusted party holds the data in usable form, relies on no intermediary.

Brain-computer interfaces represent the point where expression doctrine may reach its limit. Neural data is categorically different from other digital data. It is generated without intentional disclosure, can reveal information the person is not aware of, precedes any decision to communicate, and flows continuously as long as the device is active. Expression doctrine protects the outputs of thought and the conditions that enable those outputs. This logic suggests that expression doctrine extends to the cognitive environment in which thoughts form, even if the status of pre-expressive neural data itself remains uncertain. If expression requires privacy, and cognition is the process from which expression emerges, then the conditions under which cognition occurs are part of what expression doctrine protects. The legal doctrine that protects the right to build privacy tools has boundaries, but the tools do not. The point where expression doctrine reaches its limit is evidence that privacy ultimately needs protection on its own terms, not only as a component of expression.

Chile became the first country to amend its constitution to protect brain activity and the information derived from it, by Law No. 21.383 in 2021. Frameworks for cognitive liberty that address this frontier have been developed in legal scholarship (Farahany, 2023; Ienca and Andorno, 2017).

Protecting the right to build privacy infrastructure matters beyond blockchain because as these technologies converge, the underlying privacy problem converges with them. The same ecosystem that builds on-chain privacy is building the cryptographic foundations that AI interaction and eventual neural-data privacy will depend on.

Whether the expression argument generalizes beyond these technologies remains an open question. Privacy technologies where the expression connection breaks down would mark the limits of the argument.

Additional References for Appendix A

- Chile. Law No. 21.383, amending Article 19 of the Political Constitution of the Republic (October 25, 2021).

- Farahany, Nita. *The Battle for Your Brain*. St. Martin's Press (2023).
- Ienca, Marcello, and Roberto Andorno. "Towards New Human Rights in the Age of Neuroscience and Neurotechnology." Life Sciences, Society and Policy 13:5 (2017).
- Koi Security. "8 Million Users' AI Conversations Sold for Profit by 'Privacy' Extensions" (December 15, 2025), archived July 18, 2026: https://web.archive.org/web/20260718/https://www.koi.ai/blog/urban-vpn-browser-extension-ai-conversations-data-collection
- Salib, Peter N. "AI Outputs Are Not Protected Speech." Washington University Law Review 102, 83 (2024).
- Volokh, Eugene, Mark A. Lemley, and Peter Henderson. "Freedom of Speech and AI Output." Journal of Free Speech Law 3, 651 (2023).