COIN CENTER

April 21, 2026

Paul Atkins, Chairman
United States Securities and Exchange Commission

Hester Peirce, Commissioner
United States Securities and Exchange Commission

Dear Chair Atkins and Commissioner Peirce,

This letter addresses a threshold issue for the Commission's approach to digital assets: the First Amendment limits on SEC jurisdiction over software development, publication, and neutral web and blockchain infrastructure.

Those limits should not be left to emerge only as affirmative defenses to Commission enforcement actions. They can and should be articulated *ex ante* by the Commission itself. Without clear guidance, existing broker-dealer and exchange concepts—already broad and underdetermined—risk being applied by proximity to activities that are, in substance, the publication of software and information. In the context of modern computing, that ambiguity does not merely create uncertainty; it risks chilling the constitutionally protected speech that is at the foundation of these innovative technologies.[1]

The Commission is well positioned to address this directly by clarifying the boundary between publication and regulated conduct and by ensuring that its investigative and enforcement processes respect that line. Coin Center urges the Commission to tackle these difficult topics through an interpretive ruling on the Constitutional limits to its authority. To assist in that work, we are attaching our newly published report on the application of First Amendment jurisprudence to crypto software development alongside this letter.

[1] *See Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 713 (1931) (recognizing prior restraints as presumptively unconstitutional); *Lovell v. City of Griffin*, 303 U.S. 444, 451–52 (1938) (invalidating a licensing requirement for distributing literature); Coin Center, Software Is Speech § IV.C (2026) (explaining how licensing regimes applied to software publication raise prior restraint concerns).

The Commission's recent Staff Statement[2] concerning broker-dealer registration for certain user interfaces already points in the right direction. It distinguishes between the mere act of making software publicly available and activities involving control, discretion, or participation in user transactions. We also agree with Commissioner Peirce's associated commentary that the staff statement, while helpful, should be followed by "a more permanent regulatory approach."[3] The distinctions at play touch on the most permanent passages of American law, the Constitution, and our rights as Americans to speak and publish free from prior restraint and without compulsion to express messages preferred by the government but not the speaker.

As suggested by Commissioner Peirce, there is now an opportunity to make these principles explicit. Congress is already moving in a similar direction, with current legislative proposals urging clearer limits on registration authority consistent with the First Amendment. But the Commission need not wait for legislation. The constitutional boundary exists irrespective of any new statutory authority, and Commission-level guidance articulating that boundary would provide durable clarity to both market participants and staff.

There are two core constitutional principles ripe for clarification. First, that the First Amendment protects the publication of software, data, technical designs, and neutral communications tools. Second, that registration requirements are only constitutionally permissible as prior restraints where a person takes another's financial affairs in hand in the traditional sense of an agent, principal, custodian, advisor, or manager who is exercising client-specific discretionary authority.[4]

The first principle can be dealt with swiftly. The Commission can explicitly reject a recurring doctrinal error in this area. Some lower courts have suggested that software may receive diminished First Amendment protection because it is "functional" or capable of producing real-world effects. That approach has no basis in Supreme Court precedent. The Court has repeatedly held that the creation and dissemination of information is speech, even when

[2] Staff Statement on Broker-Dealer Registration Requirements for Certain User Interfaces, Div. of Trading & Mkts., U.S. Sec. & Exch. Comm'n (Apr. 2024).
[3] Hester M. Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, Interfacing with our Inner Demons: Comments on the Division of Trading and Markets' Statement on Certain User Interfaces (Apr. 13, 2026), U.S. Sec. & Exch. Comm'n.
[4] *See Lowe v. SEC*, 472 U.S. 181, 208–10 (1985) (White, J., concurring) (distinguishing protected publication from regulated professional conduct and explaining that a professional is one who "takes the affairs of a client personally in hand"); Coin Center, Software Is Speech § V.A (2026) (discussing the constitutional boundary between publication and client-specific advisory relationships).

that information is technical, commercially valuable, or used to guide conduct.[5] The Commission should make clear that, following binding Court precedent, it does not treat software as a lesser category of speech and does not treat the fact that software can be used to perform actions—or to facilitate activities that were historically intermediated—as a basis for diminishing First Amendment protection or expanding its jurisdiction.

With that constitutional baseline in place, the relevant question is not whether software is useful or capable of facilitating transactions, but whether a person has moved beyond software publication into a role long understood to be subject to regulation. The Commission can provide durable clarity by articulating this boundary in concrete terms.

For this, we propose an analytical framework, structured as a sequence rather than an open-ended balancing test, composed of three parts:

First, does the person have custody of, or unilateral control over, the securities or funds of others? If the answer is yes, the First Amendment limit is much weaker and ordinary regulation may apply because custody or unilateral control is a strong marker of conduct rather than publication, as a person who can seize, redirect, hold, or dispose of another's assets is in a very different posture from a publisher or infrastructure provider.

Second, even without custody, does the person *retain ongoing discretionary power* over how securities transactions are facilitated *after or alongside publication*? If not, and the person is publishing software or providing tools of general use, the activity is firmly protected by the First Amendment. Mere publication of tools that investors choose to employ to perform securities transactions does not become regulated conduct just because the tools are useful for conducting transactions that once would have required an intermediary.[6] This includes

---

[5] See, e.g., *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) (holding that "the creation and dissemination of information are speech within the meaning of the First Amendment"); *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001) ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category"); *United States v. Stevens*, 559 U.S. 460, 472 (2010) (rejecting creation of new categories of lesser-protected speech based on contemporary concerns); *303 Creative LLC v. Elenis*, 600 U.S. 570, 588 (2023) (confirming that speech is protected regardless of medium). *Cf. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449–50 (2d Cir. 2001) (suggesting that code's functionality may bear on the level of First Amendment protection); *Defense Distributed v. Att'y Gen. of N.J.*, 971 F.3d 485, 496–500 (3d Cir. 2020) (applying a context-specific inquiry into whether code is sufficiently expressive to warrant First Amendment protection). See also Coin Center, Software Is Speech, § III.B–C (explaining why these approaches depart from Supreme Court doctrine).

[6] *See Lowe*, 472 U.S. at 206–08 (holding that general investment publications are protected speech rather than regulated advisory conduct); *Taucher v. Born*, 53 F. Supp. 2d 464, 480–82 (D.D.C. 1999) (holding that requiring publishers of trading systems and software to register as commodity trading advisors violated

publishing new versions of software, recommending updates, or attempting to persuade users to adopt improved or modified tools. Those activities remain speech, even where they are effective in influencing user behavior.[7]

The relevant question is whether the person retains the ability to affect user transactions or positions without fresh user assent. The hard cases arise only where a person maintains a continuing role that allows them to alter outcomes, routes, or conditions of transactions in a way that goes beyond user-directed action.

Third, where some ongoing discretionary role is retained, is that role merely ministerial or communicative, or is it part of an agency, fiduciary, or client-specific advisory relationship of the sort described in *Lowe v. SEC*?[8]

Not all discretion is relevant in this context. Many systems involve automated processes, parameter-setting, routing logic, or the aggregation and presentation of information. Those features may influence user decisions, but they do not, by themselves, constitute the exercise of professional judgment on behalf of another.

The relevant distinction is whether the asserted discretion is exercised *for* the user in light of that user's particular circumstances, or whether it is exercised for general system design, maintenance, or communication. Where the activity consists of repackaging, organizing, or presenting public information, or providing tools that users independently employ to make their own decisions, it remains ministerial or communicative—even where the tools are highly sophisticated or effective.

This is consistent with the distinction recognized in *Lowe*, where the Court drew a line between generalized publications available to the public and conduct in which a professional takes a client's affairs personally in hand. Modern financial tools such as data terminals and analytics platforms may dramatically reduce information asymmetries and enable rapid, informed

---

the First Amendment absent individualized client relationships); Coin Center, Software Is Speech § V.A (2026).

[7] *See* Coin Center, Software Is Speech, § V.B.ii (distinguishing between (i) publication of updated software or opt-in upgrades, which remains protected speech, and (ii) retained authority to alter user positions or outcomes without fresh assent, which may indicate a shift toward regulable conduct).

[8] See *Lowe* v. SEC, 472 U.S. 181, 232 (1985) (White, J., concurring) (distinguishing regulated conduct where a professional "takes the affairs of a client personally in hand" from generalized publication); *see also Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) (recognizing that the creation and dissemination of information, including commercially valuable data, is protected speech); Coin Center, Software Is Speech, § V.B.iii (discussing user interfaces, information asymmetries, and analogies to financial data platforms).

decision-making, but their developers do not thereby become fiduciaries or intermediaries. The same principle applies here.

Where discretion operates only at this general, system-wide level, the activity remains presumptively protected. Where it instead involves delegated, client-specific judgment or authority over transactions, regulation is more plausible. The fact that a tool makes decision-making easier, faster, or more informed does not convert its publisher into a regulated intermediary.

Using this framework, an interpretive guidance should clarify that certain activities be treated as presumptively ministerial or communicative. These activities can be separated into four categories, all of which inherently contain these properties.

The first category are those activities that consist of deterministic integrity and validation functions, such as: validating digital signatures, checking transaction formatting, verifying data integrity, and enforcing deterministic protocol rules. These various activities are all mechanical checks and not professional financial judgment, and should therefore be treated as ministerial.

The second category are those activities that consist of consensus ordering and network processing, as these are incidents of network operation and communication, not agency. These sorts of activities include ordering transaction data within an open proof-of-work or proof-of-stake mechanism, block construction or validation according to open protocol rules, and routine propagation or relaying of transaction messages or blocks.

The third are those that consist of repackaging or reorganizing public information, which remain protected so long as the service does not provide individualized financial advice in light of a client's specific objectives, risk tolerance, or circumstances per *Lowe*. These activities include displaying on-chain data in more usable form, quoting observed network fees or likely fee estimates for settlement or finality, presenting liquidity, pricing, or blockchain state information derived from public sources, and assisting users in viewing and interacting with a blockchain.

The fourth and last category are those activities that consist of publishing or deploying general transaction tools. In these cases, the user initiates, chooses, and signs the transaction, and the developer or publisher does not take over the user's financial affairs. This includes publishing or deploying open-source or source-available automated market makers (AMMs), matching engines, wallet software, and routing or transaction-construction tools.[9]

[9] See Taucher, 53 F. Supp. 2d at 480–82 (holding that software and systems made available to the public do not constitute regulated advisory conduct absent individualized relationships); *Lowe*, 472 U.S. at 206–08; Coin Center, Software Is Speech § V.B.iii (2026).

Importantly, this framework would not encompass the edge cases of control and client-specific professional conduct that would move beyond First Amendment protections and into regulable conduct. Some indicators that an activity may be regulable conduct include: custody or unilateral asset control, authority to execute, alter, or block transactions on behalf of users, ongoing discretionary management of user assets or strategies, individualized financial advice tied to a client's circumstances, an agency or fiduciary relationship of trust and reliance, or bespoke services where the provider is effectively taking a client's affairs personally in hand.

It is also important to distinguish between permissible regulation of conduct that incidentally burdens speech and impermissible regulation that compels the redesign of speech itself. The Commission may regulate activities such as custody, execution, or agency relationships, even where doing so has incidental effects on how firms communicate. But where a theory of liability depends on requiring a developer or publisher to alter the design of software—such as by introducing user identification, monitoring, or intermediation functions that the software would not otherwise contain—the burden is no longer incidental. It is a direct compulsion of speech and expressive design.

The Treasury Department's 2024 non-custodial broker-reporting rulemaking illustrates the problem.[10] That proposal would have extended reporting obligations to software developers and other non-intermediaries who neither effected transactions as agents nor maintained customer relationships in any traditional sense. Because those actors did not possess the required information, compliance would have required redesigning their software to collect and report user data. In effect, the rule attempted to solve the absence of a traditional intermediary by forcing publishers of self-directed tools to become intermediaries. That move is not a regulation of conduct with incidental effects on speech; it is a compelled transformation of speech into regulated activity.

The same concern should guide the Commission's own approach. Where regulation depends on treating the publisher of a tool as the "missing middleman," and thereby requiring changes to the content or architecture of the software itself, the First Amendment is directly implicated.

Additionally, for this framework to be most effective, we recommend that the Commission build internal procedures that require First Amendment considerations before investigations escalate. This is important because constitutional limits are less meaningful if they appear only

[10] See Coin Center, Software Is Speech § V.C.ii (analyzing Treasury's broker-reporting proposal and explaining how imposing reporting obligations on software publishers would require compelled redesign of software to create intermediary functions that do not otherwise exist); *see also Nat'l Inst. of Family & Life Advocates v. Becerra*, 585 U.S. 755, 766–68 (2018) (compelled speech subject to heightened scrutiny outside narrow disclosure contexts); *303 Creative LLC v. Elenis*, 600 U.S. 570, 588–89 (2023) (government may not compel creation of speech conveying a preferred message).

as after-the-fact defenses in court, and the Commission would be better equipped to protect speech, improve staff discipline, and create a reviewable administrative record. This is especially important as the Commission may be faced with cases attempting to litigate the line between software development and regulable conduct, considering the rapid evolution of the technology. This approach would also reduce chilling effects on software development and web services, develop a clearer record of agency reasoning for the courts, avoid turning constitutional boundaries into private litigation costs, and does not require Congress or sweeping substantive exemptions.

For these reasons, Coin Center proposes implementing a checklist prior to a Wells Notice or formal action, adhering to recordkeeping and transparency, and conducting Commission-level review for edge cases.

Specifically, before opening a formal investigation premised on broker, dealer, exchange, adviser, or similar theories against a software developer, publisher, or web service provider, staff should document: whether the target had custody of securities or funds of others; whether the target had unilateral power to alter, route, block, or execute transactions; whether the target exercised ongoing discretion over transaction facilitation; whether any such discretion was merely ministerial or communicative; whether the target had an agency, fiduciary, or client-specific advisory relationship with users; whether the target used user-specific information to exercise financial judgment on behalf of users; whether the theory of liability rests on publication / infrastructure activity alone; and whether enforcement would burden protected speech, and if so whether the burden is merely incidental to regulation of conduct rather than direct regulation of publishing as such.

Staff should also create a written record of this analysis before Wells notice or comparable escalatory action. That record need not be public immediately, but it should exist so that the Commission, reviewing courts, and defendants can understand how the Commission reasoned under its own policy. And where staff believes action is warranted despite substantial speech concerns, escalation should require Commission-level or senior-level approval. This would ensure novel or aggressive theories receive scrutiny before reputationally damaging steps are taken.

To summarize, we recommend that the Commission issue formal guidance stating that the First Amendment limits SEC jurisdiction over neutral software publication and neutral web and blockchain infrastructure, and that ordinary securities regulation becomes more plausible only where agency, custody, client-specific discretion, or similar professional conduct is present. We also recommend that the Commission state that the specific categories listed above are presumptively ministerial or communicative and therefore presumptively protected absent

additional facts showing client-specific professional conduct. And lastly, that the Commission adopt an internal checklist and written-review process for investigations and Wells notices implicating software publication, web services, or blockchain infrastructure.

This approach would also be consistent with the Commission's own longstanding recognition of the constitutional limits on its authority. As Commissioner Roberta Karmel explained in 1979, there is a "tension between the First Amendment and federal securities laws" that should drive the Commission to adopt "rules in a less restrictive form."[11] That principle applies with equal force here. Where regulatory approaches risk burdening protected publication—particularly by treating software developers as if they were intermediaries—the Commission has both the authority and the obligation to adopt narrower, constitutionally sound interpretations explicitly to the public and internally through enforcement and investigatory procedures and safeguards.

Sincerely,

Peter Van Valkenburgh
Executive Director, Coin Center

[11] Roberta S. Karmel, "The Tension Between the First Amendment and Federal Securities Laws," Securities and Exchange Commission, remarks to the American Friends of the Hebrew University, September 14, 1979, https://www.sec.gov/news/speech/1979/091479karmel.pdf.

Software is Speech: Why Regulators Cannot Invent the Missing Middlemen

"i'm sorry that your warrantless surveillance regime was built on the assumption that people would always need intermediaries to transact" — unattributed

Version 1 | April, 2026

Abstract

Financial regulation has traditionally applied where a person takes another's affairs in hand—exercising custody, control, or delegated judgment. Modern software, however, allows individuals to transact directly, without intermediaries. Some regulators and lower courts have responded by advancing a "functional" theory of code, treating software as less protected speech when it is effective or capable of facilitating regulated activity.

This paper argues that approach is wrong. Writing and publishing software is protected speech, and neither its technical nature nor its usefulness diminishes First Amendment protection. Supreme Court precedent does not recognize a lesser category of "functional" speech. The constitutional line turns instead on role and relationship: whether a developer acts as an agent or exercises discretion on behalf of users.

Drawing on *Lowe v. SEC* and related cases, this paper distinguishes protected publication from regulable professional conduct and applies that distinction to core categories of crypto software. It concludes that regulators may oversee those who act as intermediaries, but may not impose prior restraints on those who merely publish the tools others use.

Authors

Peter Van Valkenburgh
Coin Center
peter@coincenter.org

Lizandro Pieper
Coin Center
laz@coincenter.org

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.

I. Introduction and Executive Summary

Under the ancient common law of agency, legal duties arise when one person is empowered to act on another's behalf and is subject to that principal's control. Early-twentieth-century legislators and regulators took this bottom-up standard, along with related doctrines of custody and fiduciary responsibility, and built a top-down licensing architecture around it: the broker, dealer, banker, or money transmitter must register because they stand in a position of trust, control, or custody vis-à-vis customers.

Cryptocurrency technology now lets anyone develop and publish software that others may use in financial transactions, yet many software developers never acquire discretionary control over user assets or undertake to act for users. They are speakers and inventors, not agents, custodians, or fiduciaries. Extending pre-registration or licensing requirements to this speech activity drops the historical logic of financial oversight and imposes a classic prior restraint on activities that are primarily speech and expression—which is almost always unconstitutional.

The Supreme Court has long rejected such extensions, even in the context of financial professionals: "One who takes the affairs of a client personally in hand and purports to exercise judgment on behalf of the client in the light of the client's individual needs and circumstances is properly viewed as engaging in the practice of a profession."[1] A publisher who does not take the affairs of a client personally in hand or exercise judgment on the client's behalf is simply speaking, not practicing a regulated profession.

This agency line does not shield developers who in fact function as agents. So-called "decentralized-in-name-only" (DINO) projects, for example, may retain "upgrade" or "administrative" keys that allow operators, in practice, to direct user assets or override user intent. In those circumstances, the developer's role may extend beyond publication into ongoing control over user affairs. But the mere existence of such powers is not enough to justify a prior restraint on software publishing. Administrative controls can be narrowly scoped, such as time-locked or multisignature controls limited to bug fixes or bounded parameter changes that cannot seize or redirect funds. In these cases, the developer has not necessarily assumed a fiduciary role. The appropriate inquiry is functional: whether the developer has undertaken to exercise judgment on behalf of users in a manner consistent with traditional agency.

Nor does the First Amendment block robust ex-post enforcement against software developers in certain contexts: fraud, deceptive-practice, and similar actions remain fully available when a tool's publisher materially misrepresents its capabilities and harms users.

[1] *Lowe v. SEC*, 472 U.S. 181, 232 (1985) (White, J., concurring in the result).

However, the First Amendment prohibits prior restraint (e.g. licensing or registration) or compelled speech (e.g. compulsory redesign of software) for developers who do no more than publish and maintain software and data. That protection does not depend on the medium of publication or the technical character of the material. Software does not lose constitutional status because it is deployed to a website, embedded in a blockchain, or written in executable form. Nor does its usefulness diminish its protection. The contrary view—that "functional" code receives lesser protection—has no grounding in Supreme Court precedent. The relevant line is crossed only when a developer moves beyond publication and assumes a role involving agency, custody, or delegated judgment over the affairs of another.

This paper will thoroughly outline the First Amendment case for software publication in four parts. First, we explain three types of crypto software: blockchain node clients, smart contracts, and user interfaces. We then identify critical distinctions in the nature of software and its publication; specifically, whether someone is publishing or running software. Second, we draw on existing First Amendment jurisprudence to distinguish between "pure speech" and "expressive conduct," and explain how merely publishing software is itself engaging in pure speech—despite its effects and the form in which it is published. Third, we identify what types of restrictions regulators seek to apply to publishing activities and their treatment under the First Amendment. Fourth, we identify ways in which a developer may also be engaged in "professional conduct," and where regulation may apply without jeopardizing the integrity of First Amendment protections.

This paper provides a framework for courts and regulators to distinguish between protected software publication and regulable professional conduct. It is intended to guide both litigation and rulemaking in an area where doctrinal clarity is urgently needed to protect American rights and technological dynamism.

II. Publishing versus Running Software

In conducting a First Amendment analysis of software, it is vital to distinguish the publication of crypto software from the running, or execution, of software. With blockchains and smart contracts, there are those who publish the software for anyone in the world to use and those who actually take the software and run it locally on their computers. This is similar to the distinction between a composer and an orchestra, or the creator of a recipe and a chef. In both instances, the publisher is merely creating and disseminating information, like instructions, for others to use. While these instructions may require the use of a computer for their execution, their dissemination is no less speech than the sharing of sheet music, which may require use of a violin for performance, or of a recipe, which requires an oven to make cake.

A. Defining Software

Oxford Dictionary of Computer Science defines "software" as: "A generic term for those components of a computer system that are intangible rather than physical. It is most commonly used to refer to the programs executed by a computer system as distinct from the physical hardware of that computer system, and to encompass both symbolic and executable forms for such programs."[2] In other words, software is one or more programs, or sets of instructions, in symbolic or executable form, used in a computer system to perform certain operations. In this report, "publishing software" means making these programs publicly available for others to use. In many court cases and legal discourse, one will find the term "code" as well as "software." We treat these terms interchangeably to describe the intangible components of computer systems.

Importantly, as we will later discuss, the First Amendment analysis does not change depending on whether software is in its symbolic form (sometimes called "source code") or in its executable (sometimes called "machine code") form. First, source and machine code are merely two ways of expressing the same thing. Source code is more easily human-readable. Compiled code is machine-readable, and may also be referred to as object code or bytecode depending on the context.[3]

Second, irrespective of whether a particular expression is encoded in source code or machine code, that software is still information, which, based on Supreme Court precedent,[4] is speech whose dissemination is protected by the First Amendment irrespective of form or language.

Third, an interpretive attempt to protect only source code and not machine code, apart from being unprecedented,[5] would create perverse regulatory results. Compiling source code into executable machine code is typically a one-step, seconds-long process using widely available tools, often requiring nothing more than a standard compiler and a single command. As a result, restricting distribution of machine code while permitting source code would be a poor policy choice, because it would do little to stop determined actors while

[2] Software, in Oxford Dictionary of Computer Science 510 (Andrew Butterfield & Gerard Ekembe eds. 7th ed. 2016).

[3] Source code is the human-readable instructions that describe what software should do. Object code is when source code is compiled to be machine-readable and able to be executed on a particular type of computer processor and operating system (OS).

[4] See infra III.A.

[5] Binding Supreme Court precedent forbids treating certain kinds of speech as subject to lesser first amendment protections unless there is historical basis for the exclusion, e.g. obscenity. See infra III.A. Lower courts have erroneously suggested that machine code should be subject to lesser protections than source code but these decisions do not identify any historical basis for those exclusions. See infra III. B.-C.

disproportionately burdening ordinary users who may struggle with the technical ability to compile software themselves. It would be like protecting religious speech only in Latin, leaving experts free to communicate while forcing ordinary people to depend on a clerical class to translate and interpret it into the vernacular.

Speaking generally, cryptocurrency technologies consist of various types of software programs, but this report will only focus on software for blockchains, smart contracts, and user interfaces. The three will fall under the umbrella term "crypto software."

B. Blockchains

There are three important components for understanding a blockchain and the peer-to-peer (P2P) network in which it exists. First is the blockchain itself, which is a cryptographically linked ledger—a type of data structure[6]—for recording information, such as transactions and other software applications known as smart contracts (more on this later). Second is the protocol, which at a high-level consists of the rules by which two or more devices interact with each other. In the context of blockchains, the protocol is the rules that determine which blocks of transactions are valid and how network participants (i.e., nodes) converge on a single canonical chain of recorded information. Third, and most important for the context of this report, is the software that a node uses to actually implement the protocol; this is known as the node client.

The first two components—that is, the blockchain data structure and the protocol—both exist within the software of the node client, allowing a node to participate in the network when running the software locally on their computer. More specifically, each node in a network runs compatible software and stores a local copy of the blockchain on their own machine (i.e., computer).[7] A node will receive a transaction that was communicated to them from a user, validate that it abides by the protocol's rules, and then relay it to peers in the network to do the same so that the transaction can eventually be packaged with other valid transactions in a block by a block proposer (e.g., miner or validator). Once this block is packaged with other valid transactions, it is relayed to the nodes to validate the block as a whole and update their local copies of the blockchain. All of this is done through operating a node client on one's own computer.

---

[6] A systematic way of organizing and storing data in a computer so that one can access, update, and process it efficiently. Specifically, a data structure determines how the data is represented; what someone can do with it; and how fast those operations take place.

[7] Full nodes independently verify blocks and transactions under the protocol's rules (often keeping a local copy of the blockchain). Other nodes, such as light clients, do not fully verify the blockchain and instead hold limited responsibilities in their network participation. For simplicity, this report uses 'node' to mean 'full node.'

Node clients are published in various locations, including public code repositories like GitHub[8] or websites specific to the blockchain, where the source code is available for any independent third-party to compile it and operate the software on their own computer. The publisher of a blockchain's node client does nothing more than write the code and publish it for anyone to use—just like publishing a recipe for others to cook a meal, or a musical composition for others to play music. In this sense, a publisher is primarily creating and disseminating information that any third-party may use; thus, the publisher does not, by publication alone, operate the network.

When a publisher makes any updates to the code, it is like when authors publish new editions of textbooks, or when the *New York Times* revises an article to improve accuracy. The decision to run certain node client software remains with network participants themselves,not the publisher. Some updates to the software allow for backwards compatibility with the existing blockchain—meaning that nodes running the old software can still work with those running the new software. In cases where updates are not backwards compatible, the network can "hard fork" if nodes do not converge on the same software—which can result in two alternative versions of a blockchain network. Even in this case, node operators who refuse to update to the newer, incompatible software are not beholden to the software developers; they can continue running the earlier version and, if other software operations make a similar choice, they will continue to have a functional peer to peer network running the older client while those upgrading have a separate functioning network with the new client software.[9] Throughout, the publisher remains in their respective role of merely publishing software and the network participants choose which software to actually operate and which networks to join.

Notably, there are certain networks in which the core developers do exercise control over who can or cannot participate as a node in the network. These are called"permissioned blockchains." Developers of these clients may be in different circumstances than those who merely publish a node client for "permissionless" blockchains, where anyone can run the client locally on their computer. In these cases, the developers may also be involved in activities beyond software publication, as they identify and interact with certain participants and control

[8] A Github repository is "a place where you can store your code, your files, and each file's revision history." In other words, a website for publishing code on the internet for anyone to review, as well as collaborate on. GitHub, *About Repositories*, GitHub Docs, https://docs.github.com/en/repositories/creating-and-managing-repositories/about-repositories (last visited Feb. 18, 2026).

[9] See Ezekiel Ologunde, Governance Models and Hard Forks in Decentralized Blockchains (2026) (hard forks "permanently split a chain" when participants fail to coordinate); see also Fork (Blockchain) (noting incompatible upgrades create two networks, one following old rules and one new); cf. The DAO (Ethereum split into Ethereum and Ethereum Classic when some participants refused the fork).

a "gating" function for determining who can or cannot participate in the network. The publication of that software may still be protected speech, but in this case there are circumstances in which professional conduct (e.g. contractual negotiations, agency relationships, or fiduciary duties) may exist. That conduct (apart from speech) may be subject to licensing, registration, or other regulation. We will later discuss these harder questions about the ability to regulate those activities versus speech.

C. Smart Contracts

A smart contract is software that has been published to the immutable ledger of a blockchain and that executes a specific function upon the request from a user, so long as the conditions written in its code are met. After the network receives the user's smart contract transaction, each full node in the blockchain network independently runs the smart contract's bytecode[10] on their computer as part of the validating process and the network's consensus mechanism determines its inclusion on the blockchain (more on this later).

The blockchain network serves as the location for storing a smart contract, much like a server acts as storage for a website or application, except that it is multiple nodes that act as "servers" with their local copies of the blockchain rather than one single server. Publishers of smart contracts write software and make it publicly available for others to use on their own by deploying it on a blockchain. It is no different than posting the code on Github or publishing it in a book, just a different medium. Deploying a smart contract consists of the following:

1. The developer writes the smart contract's source code, which is a high level language that is easier to comprehend.
2. The developer compiles, or translates, the language into bytecode, which is language that is executable in a virtual machine (VM)[11] and allows for computers in the network to "comprehend" the instructions of the code.
3. The developer deploys the bytecode to a blockchain in a transaction, where instead of inputting an amount of cryptocurrency and the wallet address of a recipient, the

[10] Bytecode is when source code is compiled to be machine-readable and able to be executed within a virtual machine—such as the Ethereum virtual machine (EVM). While bytecode and object code are both compiled source code, the two differ in where they are meant to be executed: bytecode in a VM and object code in a computer processor and OS.

[11] A virtual machine (VM) is software that emulates a computer environment that is isolated from the actual operating system of a physical computer. This provides a standardized "execution environment" for a node in the Ethereum network to run bytecode according to specific rules in the VM.

developer inputs the bytecode as structured data to store on the blockchain at a unique contract address.[12]

4. The developer signs the deployment transaction with their private key, as users do with ordinary transactions, and then broadcasts it to the network.
5. A node in the network receives the deployment transaction, validates that it abides by protocol rules, and relays it to its peers, eventually making it into a memory pool (mempool) of other transactions awaiting its inclusion in a block.
6. A block builder packages the deployment transaction with other transactions.
7. A block proposer proposes it to validators who attest the block and eventually reach consensus on it, updating their copies of the blockchain.

Once a smart contract is successfully deployed on a blockchain, it is immutable—meaning, it can't be changed or reversed, just like other transactions on a blockchain. The person deploying the smart contract is merely publishing software on a blockchain for anyone to use, while the nodes in the network have a more active role in its operability on the blockchain.

One way to think of deploying a smart contract is like publishing software on Github, which lives in a Microsoft server. The difference is that a smart contract, once deployed, lives on a decentralized P2P network and cannot be changed. In both examples, independent third-parties can take the software and run it locally on their computer to actually conduct some activity. Another way to look at it, on a physical level, is that deploying a smart contract is similar to publishing instructions in a book, which exist in various copies belonging to various individuals, who in turn are the ones independently acting upon those instructions. This is an important distinction with smart contracts: those who actually execute the smart contract's bytecode are the nodes in a network upon receiving a signed transaction from a user, not the publishers who published the original instructions. For example, on the Ethereum network:

1. A user sends a transaction to a smart contract by specifying the smart contract's address in their transaction, signing the

[12] When bytecode is deployed, there are two forms that exist at different periods of deployment and serve different functions: init bytecode and runtime bytecode. Init bytecode is the initial bytecode that the network nodes run in order to set up the smart contract for future use. Runtime bytecode is the bytecode that comes out of the execution of the init bytecode and gets stored on the blockchain after deployment–more specifically, at its on-chain address. This is the software that executes a function upon a user's request.

transaction with their private key, and broadcasting the transaction to the network.

2. The nodes in a network validate it abides by protocol rules and place it in the memory pool, or mempool.[13]
3. A block builder selects the transaction and *runs the smart contract's bytecode on their own virtual machine* with the details of the user's transaction—along with other users' transactions—to determine what the blockchain will look like after all transactions are applied, then assembles a block reflecting the updated state of the blockchain.
4. A block proposer receives the block and independently repeats the process. In doing so, the proposer now has the end state of the transactions, allowing them to update their local copy of the blockchain.
5. Once the proposer has an updated copy of the blockchain, the block with the smart contract transaction is broadcasted to the rest of the network of validators who also run the smart contract transaction—along with the others packaged in the block—and verify that the results match the proposer's results. If so, they update their copies of the blockchain, eventually reaching consensus on the end state.

Hence, there is a clear distinction between publishing code on a blockchain and taking the code to run it locally on one's machine in order to output a result. Again, it is no different than publishing a recipe for others to cook a meal, or a musical composition for others to play music. It would be analogous to an individual publishing instructions in a book and independent third-parties taking those instructions to conduct certain activities, then communicating with each other about the result of the activities in order to reach consensus—independent of the publisher.

However, there are nuances with smart contracts that warrant consideration. Smart contracts can be one specific software application within a set of various other smart contracts. These sets are often referred to as decentralized finance (DeFi) protocols. Smart contracts communicate data with each other in this set when it is encoded within each smart contract's bytecode to do so. And because of smart contracts' immutability, fixing bugs and inefficiencies in a protocol is often done in one of two ways: by either simply publishing a new smart contract

[13] A "waiting area" of valid transactions awaiting inclusion in a block to be proposed to the network.

for users to now use, or by designing a DeFi protocol to be upgradable by replacing smart contracts within the protocol using one of various design patterns.

There are also cases in which developers may wish to maintain some degree of control over the smart contract software and write privileged functions into the code. At a high level, these functions—known as administrative functions—allow authorized individuals to input certain data or requests[14] into a smart contract that would then change its behavior. This is distinct from "rewriting" the code per se, and is more so the ability to input new information to the software as it exists in order to dictate its output.[15] As mentioned, one such function is the ability to change which smart contracts are connected with each other, in turn, upgrading the DeFi protocol in order to deal with bugs and inefficiencies in the software.[16] Other functions include a fee switch and fee recipient, blacklist and whitelist authority, and token supply.[17]

The existence of upgradability or administrative functions does not itself negate First Amendment protections. As previously mentioned with node clients, this can exist in a manner similar to publishing new textbooks or revising articles based on new information. However, the presence of these administrative functions in smart contract software may indicate that the

---

[14] Sending a transaction to a smart contract is one kind of request, but in this context, a request is referring to the activities listed at the end of this paragraph.

[15] Smart contract software remains immutable, which means it can't be rewritten, compiled, and redeployed on the blockchain as the same smart contract. Once deployed, the smart contract remains that way. So core developers may write a function within the smart contract's software that allows them, or others, to input data or requests and influence the output of a smart contract.

[16] In the case of upgradability, this may allow an administrator to change which underlying smart contract users send transactions to, despite still sending transactions to the same address. A common design pattern is known as a proxy. In a proxy pattern, there exists an implementation smart contract and a proxy smart contract. The proxy contract acts as a front-facing smart contract that users and other smart contracts refer to in communicating data; the implementation contract is the underlying smart contract with the actual logic for performing a task. When upgrading in a proxy pattern, administrators may input the address of a new implementation contract into the proxy contract so that it refers to this new smart contract for all further transactions. This is may be done in good faith in order to maintain consistency for users so they may continue directing their transactions to the same smart contract address, and only when authorized by a decentralized governance mechanism—in which token holders of a DeFi protocol vote and approve the upgrade, then appoint a third party to deploy a new smart contract and input the new implementation contract address in the proxy. However, this isn't always the case and the privilege to upgrade the implementation contract may exist with core developers that act independently, raising regulatory questions.

[17] A fee switch is the ability to enable and disable a fee collection upon use of the smart contract and direct those fees to a specific wallet address. Blacklist authority is the ability to input which wallet addresses are blocked from using the smart contract; whitelist authority is the ability to input which wallet addresses are approved to use the smart contract. Token supply function is the ability to determine how many tokens are minted (created) or burned (destroyed), or by setting rules that control issuance of tokens.

developer has engaged or is engaging in professional conduct rather than mere speech, which we will discuss later.

Additionally, setting aside the First Amendment questions, administrative control over aspects of a smart contract should trigger separate statutory analysis to determine whether or not some sort of conduct exists that is already regulated, e.g. when acting as a securities broker (the administrative function allows the developer to play a key role in how the smart contract distributes user funds and securities) or a money transmitter (the administrative function allows the developer to accept and transmit currency substitutes). For the purposes of the First Amendment, this paper begins by focusing on smart contracts that are "written in stone" and do not authorize administrative capabilities—which is a common and often default practice in crypto.[18] After that discussion, we will address more difficult questions dealing with upgradeable or alterable smart contracts wherein the developer retains some ongoing control and, potentially, a regulatable course of professional conduct.

D. User Interfaces

There are various forms of crypto user interfaces (UI) which warrant distinct analysis under the First Amendment. But before diving into each of these, we must first understand what generally constitutes crypto UIs to properly distinguish between speech and conduct.

First, every UI is just software that acts as an interface, or display, and presents information through the form of a website or application. Some go beyond just that and allow for interactivity, or even provide services—for these we need to make distinctions. Second, every UI welcomes user inputs that affect the display of information, which means they are not static but interactive, and some welcome inputs that do more. Third, there is software that is running somewhere. This can be client-side (i.e., on the user's computer) or server-side (i.e., on a company's server). Fourth, each UI has a distribution mechanism. This can include traditional web hosting, which typically involves a domain (i.e., a website's public name) and hosting infrastructure such as servers. It can also include decentralized methods, such as IPFS, a P2P protocol for publishing and sharing files without reliance on a single server.[19] Fifth, each UI has data sources where it derives its information. The nature of a UI's data

[18] Examples include the core smart contracts in the Tornado Cash protocol (i.e., the privacy pools) which could not be changed within the protocol to ensure its security and integrity. Whereas, auxiliary smart contracts—which are not critical to the protocol—were replaceable via a proxy pattern and through a governance vote. Peter Van Valkenburgh, Amanda Tuminelli & Lizandro Pieper, *Expert Report of Coin Center and DeFi Education Fund* 13–16 (May 16, 2025), https://www.coincenter.org/app/uploads/2025/06/2025-05-16-Pertsev-Brief-Pertsev-FINAL.pdf.
[19] IPFS Docs, *What Is IPFS?* (Defining IPFS), https://docs.ipfs.tech/concepts/what-is-ipfs/#defining-ipfs (last visited Mar. 11, 2026).

dependencies—especially whether transaction-relevant functions rely on operator-controlled services—often helps distinguish a purely informational UI from a service-layer UI that allows the provider to materially shape user options, routing, or transaction execution (more on this later). Sixth, UIs include default settings, meaning preselected configurations that operate the same way each time unless the user changes them. Some default settings include the blockchain network or networks the UI reads from, the remote procedure call (RPC) endpoint for reading and broadcasting information, the routing behavior, and so on.

These characteristics and components provide a useful guide for understanding a crypto UI and where it may lie between constitutionally protected speech and professional conduct. In this regard, we will go over three forms of UI: purely informational, user-controlled, and operator-controlled UI.

i. Purely Informational UI

At the most basic level, UIs can be purely informational. This means that the interface solely takes a blockchain's publicly-available data and organizes it so users can read it more intuitively, for example blockchain explorers, which simply provide a user-friendly interface for exploring data on a blockchain. This data may include balances, transactions, and prices, but can also include more detailed information on DeFi protocols, such as bytecode and parameters (e.g., fees, trading limits, and governance).

User inputs are limited to functions that allow for searching and filtering data. Users cannot communicate transactions to the blockchain network, they can only fetch data. This means that the provider's discretion is merely editorial. That is, they decide which information users can read through their UI, much like the editor of a newspaper or newsletter that provides financial information on the stock market. Hence, as explained later, making this type of UI publicly available is constitutionally protected speech.

ii. User-Controlled UI

Another common UI is one in which users can connect their wallets, configure transactions, and sign them locally on their own computer (i.e., client-side), before broadcasting them to the blockchain network. Most UIs are categorized as "client-side," meaning the software runs on the user's computer—either as a downloadable application, a browser-based web application, or browser extension—even when the UI was delivered through a hosted website (i.e., maintained by a third-party). Because many UIs execute client-side—even those with significant dependencies on a backend (discussed in the next subsection)—we'll refer to the UIs in this subsection as "user-controlled UIs."

In this context, the UI provider is neither custodying assets on behalf of users nor executing transactions. The UI is just a software tool for users to leverage in conducting their own financial activities. The provider is best characterized as a publisher of instructions that users can operate locally on their computer. Agency exists with the user, as they are the ones signing transactions with their private keys and using the software to configure transactions, including amounts, routes, and slippage.

Another key distinction compared to the purely-informational UI is that these user-controlled UIs allow users to communicate transactions to a blockchain network, through an RPC endpoint. An RPC endpoint is the access point (typically a web address, or URL) through which a user can communicate with a blockchain node (via the UI) to read blockchain data and broadcast transactions to the network. Purely-informational UIs also use RPC endpoints to read data, but because these UIs do not allow for communication of transactions and only communicate with the blockchain network to fetch data, these UI do not raise the same concerns.

What does require further analysis, however, is when RPC endpoints are used to communicate transactions to a blockchain network. In these cases, it is important to know that RPC endpoints may be operated by the user (running their own node), by third-party infrastructure providers (e.g., Alchemy or Infura), or by the provider of the UI. This means that the chosen endpoint can function as a chokepoint where requests (e.g., transactions) are observed, rate-limited, or refused, particularly when a UI's software is hard-coded to only allow for communications through a single RPC endpoint rather than allowing the user to choose.

This is important for a First Amendment analysis because it determines where agency exists in communicating transactions: either with the user when running their own node or when choosing which provider to use, or with the provider of the UI themselves, effectively introducing a degree of discretion (despite not custodying or controlling users' private keys). With the former, the UI is a software tool for users to operate locally on their computer for conducting their own transactions, and the provider of the UI is, again, publishing computer instructions for third-parties to use. Where a UI provider acts as the RPC endpoint and exercises a degree of control, the provider is no longer just a publisher, but also an active participant in the transaction process (this will be discussed in more detail in Section V). For the sake of clarity in this report, "user-controlled UIs" will only refer to UIs in which users exert full agency and are not dependent on the UI developer for any services. The latter will be discussed in the next subsection.

iii. Operator-Controlled Service Layer

As previously mentioned, delivery of a user-controlled UI may be done through a hosted website. This is essentially publishing the interface for others to use on a website that is maintained by the provider. This allows a UI provider to more easily make updates to the UI's software so users can receive the most recent version of its code. Similar to updates to blockchain node clients, this may be editorial in nature, and is like when authors publish new editions of a textbook, or when a newspaper updates an article. The provider is acting as a publisher and merely hosting the location where their publication is delivered.

This is distinct from actually *operating* the UI, which requires running the backend service layer. We'll refer to this type of UI as a "service-layer UI." With this type of UI, the operator may control parts of the infrastructure to provide a service, despite the UI often running client-side. The distinction here between a user-controlled UI and a service-layer UI is that the former uses publicly-available infrastructure as its source of truth (i.e., a blockchain). User-controlled UI providers design the software to be read and display blockchain data, but also so users can communicate data back to the blockchain with their private keys. This means agency lies with the user (with nuances as explained earlier) and the provider merely publishes the computer instructions needed to do so. Whereas a service-layer UI may be dependent on backend infrastructure that is controlled by one party for its source of truth and operations—even if a blockchain remains the underlying ledger from which information is read and to which transactions are ultimately communicated.

In the context of the First Amendment, the important considerations to be made are: 1) whether the UI provider is publishing software or operating a service; 2) where user agency exists; and 3) whether any backend service is essential or can be bypassed (i.e., the user can refuse it for alternatives). As with our discussion of RPC endpoints in the previous section, in cases where the backend is required and allows the provider to steer or block transactions, then the provider is not merely a publisher, but also an operator. In that sense, this is no longer only an analysis of their First Amendment rights to speak, but also an analysis of potential statutory obligations on their course of professional conduct.

One example of a service-layer UI in crypto is a swap aggregator that depends on a backend application programming interface (API).[20] A swap aggregator is a service that searches across multiple venues (i.e., decentralized exchanges and liquidity pools) to find a swap route for a given trade, often splitting the order across venues to improve execution of the transaction. There are a variety of ways to go about designing a swap aggregator, and in some instances, smart contracts are used to determine best execution. In this example, however, the

[20] An API is a software interface, or connection, between different computers or computer programs.

UI may run on a user's browser, but the provider can steer outcomes through the API by changing route logic for transactions, excluding certain liquidity pools or exchanges, or refusing to serve routes. Thus, the distinction between publishing and running software is again introduced.

E. Summary

To summarize, the three forms of crypto software we will address are blockchain node clients, smart contracts, and UIs. For purposes of the First Amendment, we evaluate the act of publishing these types of software as information, or instructions, that independent third-parties such as blockchain nodes or users operate on their computers. This is relevant to our First Amendment analysis because publishers are distinct from the actual operations of the software and are merely engaged in the act of making information publicly available and, at times, are expressing a social or political message through this information.

As we later discuss, the Supreme Court has ruled favorably towards the creation and dissemination of information, and has long protected it as pure speech despite its effects and the form in which it is published. Based on that precedent, merely publishing these various forms of crypto software is entitled to the same protection. In congruence with its categorization as pure speech, we also evaluate the limitations on government to restrict publication or compel only certain types of publication through a licensing and registration regime.

Additionally, to address more complex activities beyond just publication, we evaluate the distinction between speech and professional conduct. Software developers do not always exist as mere publishers of open-source software and may participate in additional activities that may or may not warrant licensing and registration. We believe it necessary to address that distinction and protect the integrity of First Amendment protections.

III. Pure Speech versus Expressive Conduct

The First Amendment protects expression, but not all forms are protected equally. Over centuries of caselaw, the Supreme Court has drawn a foundational distinction between speech (words, images, data, or other communicative content) and conduct (physical acts that carry communicative elements, such as flag burning or nude dancing).

This speech versus conduct distinction is not academic, but legal; it determines the level of constitutional scrutiny that a government regulation receives from courts. Regulations targeting conduct that incidentally burden expression may survive under intermediate scrutiny;

for example, it is constitutional to ban the burning of draft cards.[21] But regulations targeting speech itself, such as prior restraints (e.g. licensing requirements for newspapers[22]) or compelled expression (e.g. a mandatory pledge of allegiance for public school students[23]), trigger the highest constitutional standard of strict scrutiny and are almost always found to be unconstitutional.

Those unfamiliar with the recent history of software publishing and the First Amendment may assume that the speech-conduct distinction matters only for persons engaged in more than mere software development and dissemination; such as those who publish software but *also* maintain servers, take user information, custody user funds, or control admin keys to smart contracts. It is certainly true that the line between speech and conduct is highly relevant in resolving the constitutional limits of regulations for these grey areas of publishing-plus activities. However, the speech-conduct distinction is also relevant in the simpler case of mere software publication and dissemination alone. For some lower courts, merely sharing a CD-Rom or hosting a file for download is treated as conduct rather than speech.

Lower court confusion over the distinction between conduct and speech naturally found in software publishing has fueled the development of what might be called a "functional code" theory of diminished First Amendment protection. Some courts have suggested that because software can be executed to produce real-world effects, it resembles conduct rather than speech. Others have drawn unstable distinctions between source code and object code (one communicates software ideas in human-readable form, the other in machine-readable instructions), or between software that renders expressive content (like an e-book or video game) and software that produces physical or transactional outputs (e.g. payments or 3D-printed gun parts). These distinctions often rest on the intuition that software "does things" in the world and therefore should be treated differently from other forms of publication.

Further complicating matters, the Supreme Court has never affirmed or agreed with any of the distinctions these lower courts have made; instead, the Supreme Court's modern First Amendment jurisprudence contains a consistent line of cases establishing that the creation and dissemination of any kind of information (presumably software included) is speech within the meaning of the First Amendment.

---

[21] *United States v. O'Brien*, 391 U.S. 367 (1968).
[22] *Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931).
[23] *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943).

The remainder of this section will focus on software publication alone, why Supreme Court precedent suggests these activities warrant full protection as "pure speech," and why the lower court "functional code" theory of diminished protection is aberrant, unprecedented, constitutionally unsupported, and ahistorical. We argue that where a developer merely writes and makes software available for others to use—whether by posting source code to a repository, deploying bytecode to a blockchain, or hosting a non-custodial interface—the activity at issue is the creation and dissemination of information. We argue that such activities are pure speech and that the Supreme Court's existing jurisprudence insists on this interpretation even if some lower courts have gone astray. Moreover, the fact that these publications may be easily used by others to engage in regulated conduct has no bearing on whether the published software is speech worthy of full protection. A well-drawn blueprint allows speedier and easier construction and a well-designed piece of software allows instant functionality. Indeed, the notion that we would begrudge publishers strong protections because their publications were too effective at allowing others to turn speech into action is decisively anti-intellectual and inapposite to the goals of the First Amendment.

Separately, where an actor exercises discretionary control over user assets, executes transactions on behalf of clients, or undertakes fiduciary responsibilities, the analysis shifts to professional conduct and agency law, which we address later in this report.

We will begin this section with a careful look at how the Supreme Court has characterized the publishing and disclosure of information and why software publication is, therefore, pure speech. We'll then proceed to a discussion of conflicting opinions at the lower court level. We will show that these aberrant cases lack precedent or basis in actual constitutional authority and stem from a categorical misunderstanding of software itself.

A. The Supreme Court's Lineage: Publishing Information Is Pure Speech

The Supreme Court's modern jurisprudence contains a consistent line of cases establishing that the creation and dissemination of information is speech within the meaning of the First Amendment. The Court has consistently reached this conclusion even in cases where the underlying information is dry, commercial, functional, and digital. Three cases are particularly important: *Bartnicki v. Vopper* (2001), *Sorrell v. IMS Health Inc.* (2011), and *303 Creative LLC v. Elenis* (2023). A fourth case, *United States v. Stevens* (2010), is important for an associated principle: that all types of speech are equally protected but for certain historical categories—obscenity, defamation, incitement, and a few others—and that new categories of lesser-protected speech may not be invented based on contemporary concerns or functional characteristics. Taken together, these cases pose a substantial barrier to attempts by lower courts (in cases we will review in the next subsection) to treat software as lesser-protected speech by virtue of its functionality or threadbare expressivity.

i. *Bartnicki*: Disclosure Is Speech

Bartnicki concerned the interception and recording of a phone call between union negotiators during a labor dispute, which the interceptor then shared with others, eventually reaching a radio commentator.[24] The chief union negotiator, Bartnicki, sued Vopper, the radio commentator, under federal and state wiretap laws that impose liability for disclosure of illegally intercepted communication.[25] The Supreme Court ruled that, despite interception being unlawful, Vopper was entitled to First Amendment protections for the disclosure of information that was a matter of public concern.[26] Importantly, the Court had to grapple with two foundational questions: first, is the unauthorized disclosure of illegally obtained information speech or is it conduct? Second, how does the Constitution resolve the inherent conflict between the need to protect individual privacy and the First Amendment value inherent in free disclosure of information that is of public concern?

On the first question of whether or not disclosure is speech, the Court was unequivocal. The government argued that disclosure of illegally obtained information could be regulated as conduct rather than speech. The Supreme Court rejected that premise. It explained:

> "[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct."[27]

On the second question of privacy versus disclosure, the Court sided with disclosure, finding that, since the publisher was not also the interceptor of the private conversation, a "law-abiding possessor of information" cannot be suppressed in order to "deter conduct by a non-law-abiding third party."[28]

In other words, the Court held in *Bartnicki* that dissemination of information is speech and that a law that regulates conduct by prohibiting wiretapping could not be extended to hold subsequent republishers of information liable. Wiretapping is conduct and constitutionally regulable; publishing tapped information is speech and cannot be constitutionally prohibited. Attempts to police one person's bad conduct must not spill over into prohibitions on another person's right to publish pure speech.

ii. *Sorrell*: Information Is Speech, Even When Bland and Instrumental

[24] *Bartnicki v Vopper.*, 532 U.S. 514-515 (2001).
[25] *Id*. at 514.
[26] Based on the Court's precedent in *New York Times Co. v. United States* (1971). *Id*. at 515-516.
[27] *Bartnicki*, 532 U.S. at 527.
[28] *Id*. at 529-530.

In *Sorrell*, Vermont enacted a statute restricting the sale and use of prescriber-identifying data for pharmaceutical marketing,[29] characterizing the data as a commodity subject to economic regulation.[30] The Supreme Court responded with language that bears directly on attempts to carve out "functional" information from First Amendment coverage:

> "This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment. See, *e.g., Bartnicki*… Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes."[31]

The Court acknowledged that Vermont sought "an exception to the rule that information is speech," and it declined to create one.[32] The Court additionally found that even if one assumed, *arguendo*, that the data could be treated as a commodity, the statute nonetheless imposed content- and speaker-based burdens that triggered heightened scrutiny.[33]

The information in *Sorrell* was not a symphonic score, a navigational chart, or even a particularly beautiful, but functional, architectural diagram. It was dry, commercially valuable, and behavior-influencing data about which doctors were prescribing which drugs. No reasonable human would read it for pleasure or casual edification. It was bought and sold in markets and used to affect prescribing practices.[34] If that functional or instrumental capacity diminished First Amendment protection, the Court in *Sorrell* would have said so. It did not.

iii. *303 Creative*: Online Speech and Medium Neutrality

303 Creative went a step further in developing more specific guidance for what the Court deemed "pure speech" in the context of the Internet. Here, the Court ruled that Colorado could not force Lorie Smith, a website designer for weddings, to create websites displaying messages with which she disagrees.[35] The Court reasoned that, based on Smith's stipulations, her website designs were pure speech because they 1) would contain words, images, symbols, and other modes of expression; 2) would be her original, customized creations; and 3) would be created to

---

[29] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 557 (2011).
[30] *Sorrell*, 564 U.S. at 570.
[31] *Id*.
[32] *Id*. at 571.
[33] *Id*. at 552.
[34] *Id*. at 555-557.
[35] *303 Creative LLC v. Elenis*, 600 U.S. 570, 581 (2023).

communicate her own ideas on a societal matter—in this case, marriage.[36] And because of this, the State compelling her to express a viewpoint other than her own would be a violation of the First Amendment (compulsion will be discussed fully in Section IV).

Importantly for our purposes, the Court also clarified that the format and medium of speech was irrelevant to a First Amendment analysis, stating: "All manner of speech—from 'pictures, films, paintings, drawings, and engravings,' to 'oral utterances and the printed word'—qualify for the First Amendment's protections; no less can hold true when it comes to speech like Ms. Smith's conveyed over the Internet."[37]

iv. *Stevens*: No New Categories Without History

Finally, in *Stevens*, the Court rejected an attempt to recognize depictions of animal cruelty as a new category of unprotected speech. The Court held that the First Amendment's historically recognized exceptions, such as obscenity, defamation, and incitement, cannot be expanded by judicial balancing of social costs.

This principle is critical. Courts may not invent new categories of lesser-protected speech based on contemporary concerns or functional characteristics. Any carveout must be grounded in historical tradition.

Together, these cases establish a coherent rule: publishing information—whether factual, commercial, digital, or technical—is speech. The Supreme Court has repeatedly refused to create new functional exceptions to that rule.

v. The Court's Consistent Treatment of the Dissemination of Information as Speech

The Court's cases also make clear that the First Amendment protects the dissemination of information even when that information exists primarily to guide practical or economic conduct. The Court has repeatedly rejected the idea that speech loses constitutional protection simply because it is instrumental or intended to enable action.

In *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council* (1976), the Court struck down a law prohibiting pharmacists from advertising prescription drug prices.[38] The state argued that price advertisements were purely commercial activity designed to facilitate consumer purchasing decisions.[39] The Court rejected that reasoning and held that the

---

[36] *Id*. at 571.
[37] *Id*.
[38] *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976).
[39] *Id*. at 760-62.

First Amendment protects the communication of truthful price information because "the free flow of commercial information is indispensable."[40] The fact that the information was intended to guide economic decisions did not remove it from the scope of the First Amendment.

In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.* (1985), the Court likewise treated a credit report containing technical financial information as speech for First Amendment purposes.[41] Although the Court held that the report involved a matter of purely private concern and therefore received reduced constitutional protection in the defamation context, it did not question that the publication of such financial data constituted speech.[42]

Similarly, in *Rubin v. Coors Brewing Co.* (1995), the Court struck down a federal law prohibiting brewers from displaying alcohol content on beer labels.[43] The government argued that the restriction was justified to prevent "strength wars" in beer marketing.[44] The Court rejected the regulation, holding that suppressing truthful factual information on product labels violated the First Amendment.[45]

And in *Lowe v. SEC* (1985), the Court held that publishing an investment newsletter did not constitute regulated professional conduct but instead constituted protected speech.[46] The Court distinguished between a professional who takes a client's affairs "personally in hand" and the publication of general advice to the public at large.[47] The Court's analysis recognized that the publication of investment advice, even if intended to guide financial decisions, remains protected speech. As discussed later in this report, *Lowe*'s distinction between professional conduct and general publication provides an important framework for analyzing attempts to regulate software developers and publishers.

Taken together with the Court's decisions in *Bartnicki*, *Sorrell*, and *Stevens*, these cases illustrate a consistent doctrinal principle: the First Amendment protects the creation and dissemination of information even when that information serves an instrumental purpose.

The Court has repeatedly treated the following categories of information as speech:

Type of Information	Case	Holding

[40] *Id*. at 765.
[41] *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985).
[42] *Id*. at 762–63.
[43] *Rubin v. Coors Brewing Co.* 514 U.S. 476 (1995).
[44] *Id*. at 479.
[45] *Id*. at 481-482.
[46] *Lowe*, 472 U.S. 181, 232 (1985) (White, J., concurring)
[47] *Id*. at 210–11 (1985); Id. at 232 (White, J., concurring)

Prescription drug prices	*Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council* (1976)	Advertising truthful price information is protected speech
Pharmaceutical prescribing data	*Sorrell v. IMS Health Inc.* (2011)	Creation and dissemination of data is speech; restriction unconstitutional
Recorded communications (illegally intercepted by another party)	*Bartnicki v. Vopper* (2001)	Disclosure of truthful information is protected speech
Credit reports	*Dun & Bradstreet v. Greenmoss Builders* (1985)	Credit reports constitute speech, though involving private matters
Product label information (alcohol content in beer)	*Rubin v. Coors Brewing Co.* (1995)	Government may not suppress truthful factual labeling information
Investment advice newsletters	*Lowe v. SEC* (1985)	Publishing general financial advice is protected speech

Across these decisions, the Court consistently treats the publication of information as speech even when the information is technical, commercial, or intended to guide real-world conduct. The First Amendment does not distinguish between expressive information and effective information. Once the government regulates the dissemination of any knowledge, constitutional scrutiny applies.

B. The Emergence of the Functional-Code Theory

The modern articulation of the functional-code theory of lesser constitutional protection appears most clearly in the Third Circuit's recent decision in *Defense Distributed v. Attorney General of New Jersey* ("*Defense Distributed*") which we will discuss in depth in the next sub-section. In that case, the Third Circuit did not deny that code can be speech, nor did it create a categorical exclusion for software from First Amendment coverage. Instead, it adopted a contextual framework in which certain characteristics of code—particularly whether its execution produces expressive output or non-expressive physical effects—bear on the level of constitutional protection afforded to its dissemination.

This approach reflects the culmination of doctrinal drift that began in the encryption export, copyright, and products liability cases of the 1990s and early 2000s.

i. The Encryption Cases: Code Is Speech

In *Bernstein v. U.S. Department of Justice* (9th Cir. 1999), a graduate student challenged federal restrictions that treated encryption source code as a munition requiring export licensing.[48] The Ninth Circuit held that source code is speech,[49] reasoning that code is written in a language, communicates ideas to programmers, and can be read and understood by humans. The court explicitly rejected the government's argument that code was merely functional conduct.[50]

Similarly, in *Junger v. Daley* (6th Cir. 2000), the Sixth Circuit held that computer source code is protected speech because it communicates information and ideas to those who understand the language.[51] The Sixth Circuit emphasized that the fact that code can be executed does not strip it of expressive character.[52]

These cases were doctrinally sound in recognizing code as speech, but they introduced an instability that later courts would exploit. Both opinions acknowledged that code is not merely expressive, it also leads to functionality. It can be compiled and executed. While the courts in encryption cases ultimately rejected the government's efforts to classify code as conduct, they left open the conceptual space for later courts to emphasize functionality as constitutionally significant. Thus, the earliest cases correctly held that code is speech, but they also planted the seeds of the "speech-plus-function" framing.

ii. *Corley*: Function and Value Determine Scrutiny

That framing took on sharper form in *Universal City Studios v. Corley* (2d Cir. 2001) ("*Corley*"), which upheld aspects of the Digital Millennium Copyright Act prohibiting distribution of DVD decryption code.[53] In *Corley*, the Second Circuit acknowledged that source code communicates ideas but emphasized its capacity to perform functions when executed, and suggested that code's ability to "instantly" cause decryption distinguished it from traditional written instructions.[54] The Second Circuit did not deny that code is speech, instead, it treated code's functionality as relevant to the level of protection: regulations targeting functional code that enabled illegal decryption (among other conduct) faced only intermediate scrutiny.[55]

---

[48] *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1136 (9th Cir. 1999), withdrawn, 192 F.3d 1308 (9th Cir. 1999).
[49] *Id.*
[50] *Id.*
[51] *Junger v. Daley*, 209 F.3d 481, 484–85 (6th Cir. 2000).
[52] *Id.*
[53] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).
[54] *Id.*
[55] *Id.*

But that reasoning subtly altered the constitutional inquiry. Rather than asking whether the government was regulating publication (speech) or conduct, the Second Circuit asked whether the published material could be used to accomplish conduct efficiently. That shift collapses a basic distinction. All instructions are written because they can be acted upon. The First Amendment has never conditioned protection on the speed or precision with which speech can be implemented into action. Nevertheless, *Corley* became the doctrinal foundation for these functional distinctions.

Additionally, and more subtly, the Second Circuit in *Corley* infused their analysis with normative judgment. The functionality at issue was not neutral. The software facilitated copyright circumvention and, in the Second Circuit's view, piracy. The perceived social harm of the code influenced the Second Circuit's willingness to treat its functionality as constitutionally weighty.

This values-laden framing is particularly unprecedented and ahistorical. The First Amendment does not calibrate protection based on judicial assessments of a work's social utility. In *Stevens*, the Supreme Court expressly rejected the idea that courts may create new categories of lesser-protected speech by weighing value against harm.[56] In *303 Creative*, the Court was explicit that the First Amendment protects speech even when the government finds the message objectionable.[57] Justice Gorsuch wrote:

> "The First Amendment's protections belong to all, not just to speakers whose motives the government finds worthy. Under Colorado's logic, the government may compel anyone who speaks for pay on a given topic to accept all comers and all messages. But the First Amendment protects an individual's right to speak his mind regardless of whether the government considers his speech sensible and well intentioned or deeply 'misguided.'"[58]

In *Roth v. United States* (1957), the Court held obscenity unprotected, but in doing so it made clear that:

> "All ideas having even the slightest redeeming social importance — unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion — have the full protection of the guaranties, unless excludable because they encroach upon the limited area of more important interests."[59]

---

[56] *United States v. Stevens*, 559 U.S. 460, 470–72 (2010).
[57] *303 Creative*, 600 U.S. at 595.
[58] *Id.*
[59] *Roth v. United States*, 354 U.S. 476, 484–85 (1957).

And in *Bartnicki*, the court explicitly declined to hold an innocent republisher of speech guilty for the sins of a wiretapper.

The Supreme Court has repeatedly said that speech may fall outside the First Amendment only if it fits within historically recognized and narrowly defined exceptions: obscenity, defamation, incitement, and true threats. Not "speech that facilitates something the state dislikes." Not "speech that is highly technical." Not "speech that others rely on to engage in regulated or illegal conduct."

Yet *Corley*'s analysis implicitly did exactly that. It treated decryption code as speech, but speech of a diminished constitutional stature because of the conduct it enabled and the policy interests it threatened. In *Corley,* software was not just functional; it was functionally *dangerous* and pushed into a new speech category of lesser constitutional significance.

That move planted the seed for a broader doctrinal drift. If code that facilitates copyright circumvention may be treated differently because of its functional harms, then code facilitating other controversial activities might also be treated differently.

iii. *Winter*, Post, and the "Technical Tool" Narrative

Another line of reasoning over "functional" speech emerged from *Winter v. G.P. Putnam's Sons* (9th Cir. 1991), a products-liability case involving a field guide to edible mushrooms. In distinguishing books from aeronautical charts, the Ninth Circuit described charts as "highly technical tools" and analogized them to compasses, suggesting they are more like products than expressions.[60]

Importantly, *Winter* did not conduct any binding First Amendment analysis of navigational charts, it simply contrasted books and charts for illustrative purposes. *Winter* does not hold that navigational charts fall outside constitutional protection. It addressed strict liability in tort, finding that books were not products and that strict liability for factual inaccuracies, even in the decidedly deadly context of poisonous mushrooms would not pass constitutional muster.[61]

Winter was about books and mushrooms, yet later courts, and commentators, repurposed its speculative dicta about charts and navigation. Most notably, Professor Robert Post speculated that navigational charts *might* not receive First Amendment protection because

[60] *Winter v. G.P. Putnam's Sons*, 938 F.2d 1033, 1036 (9th Cir. 1991).
[61] *Id.*

they "invite" reliance rather than dialogue.[62] That academic speculation has been cited to suggest that certain technical materials are tools rather than speech.

But there is *not a single Supreme Court decision* recognizing a "technical tools" exception to the First Amendment. Indeed, under *Stevens*, such a category would require historical grounding. None exists for navigational charts, engineering schematics, software code, or any other important technical or functional speech. This "tool versus expression" framing therefore rests on thin analogy and academic commentary alone, not on constitutional precedent.

Over time, these strands—encryption-era acknowledgment of functionality, *Corley*'s emphasis on operational immediacy and attendant illegal conduct, and *Winter*'s tool analogy—merged into a broader intuition: that code which facilitates non-expressive or illegal conduct may warrant lesser protection than code that produces expressive output.

This intuition reflects a categorical confusion. It treats speech that enables conduct as if it were itself conduct. But the First Amendment has never drawn that line. The Constitution protects books that enable chemistry, manuals that enable engineering, and treatises that enable finance. The fact that information can be relied upon does not convert publication into performance, nor turn speech into conduct.

iv. The Convergence: Function Plus Normative Judgment

By the early 2000s, two threads had merged. First, from the encryption cases and *Corley*: the idea that functionality bears on constitutional status. Second, from *Winter* and academic commentary: the idea that certain technical materials are tools rather than speech.

These threads share a deeper error. They treat the consequences of speech as constitutionally transformative. If speech enables conduct that courts view as socially harmful or important to the regulatory state, its functional character becomes suspect. If speech invites reliance rather than debate, it becomes tool-like.

But Supreme Court precedent explicitly rejects this move. *Bartnicki* held that the disclosure of facts is speech even when it causes harm. *Sorrell* held that commercially valuable, behavior-influencing data is speech even when it is utterly dry and serves only the interests of pharmaceutical marketing. *303 Creative* confirmed that software-based expression is protected irrespective of medium. And *Stevens* forbids courts from creating new categories of lesser-protected speech based on contemporary judgments of harm.

---

[62] Robert C. Post, *Participatory Democracy and Free Speech*, 97 Va. L. Rev. 477, 482–83 (2011) (distinguishing speech that participates in public discourse from technical or professional communications that guide conduct and "invite reliance").

The lower court drift meanwhile reflects two related confusions: a categorical confusion (speech that enables conduct is treated as conduct) and a values confusion (speech deemed socially harmful is treated as less worthy of protection). As we discuss in the next section, these threads have recently culminated in *Defense Distributed*.

C. Defense Distributed

In *Defense Distributed*, the appellant, Defense Distributed, published "computer files that allow anyone with a 3D printer… to produce a fully functional, single-shot plastic pistol."[63] Despite the Attorney General of New Jersey issuing a cease and desist, files could be directly downloaded from Defense Distributed's website or delivered as USB drives and SD cards.[64] New Jersey later passed legislation that made it a crime for:

> "a person to distribute by any means, including the Internet, to a person in New Jersey who is not registered or licensed as a manufacturer… digital instructions in the form of computer-aided design files or other code or instructions stored and displayed in electronic format as a digital model that may be used to program a three-dimensional printer to manufacture or produce a firearm, firearm receiver, magazine, or firearm component."[65]

Defense Distributed argued that the files were not functional or self-executing but were merely stored information, and that the files concerned "technical, scientific, artistic, and political" matters.[66] The Third Circuit did not rule on the matter outright, choosing instead to throw the case back to the lower court for more fact finding. In that order, the Third Circuit conceded that computer code *could be* covered by the First Amendment, but insisted that coverage could not be assumed in the instant case because the relevant code might be inherently functional and therefore subject to lesser or no protection.[67] As such, the Third Circuit developed a "fact-based and context-specific" analysis to determine whether or not any given computer code could be entitled to First Amendment protections. The analysis consisted of five prongs: first, whether the code is source or object code; second, how the code is used; third, the nature of the communication, and whether it is between humans or between human and machine; fourth, the code's purpose; and fifth, if and what it communicates.[68]

---

[63] *Def. Distributed*, slip op. at 2.
[64] *Id*. at 4.
[65] *Id*. at 9.
[66] *Id*. at 37.
[67] *Id*. at 30.
[68] *Id*. at 34.

In creating this test, the Third Circuit relied heavily on an unusual reading of *Bartnicki*. Recall that *Bartnicki* established the premise, later reaffirmed in *Sorrell*, that the disclosure of any kind of information of whatever form or content is pure speech. How, then, did *Bartnicki* become support for *Defense Distributed*'s opposite conclusion that disclosing some types of information was unprotected? The Third Circuit emphasized that in *Bartnicki,* the Supreme Court described the delivery of the intercepted recording as "like the delivery of a handbill or a pamphlet," and noted that the underlying wiretapped conversation concerned a public issue.[69] From this, the Third Circuit concluded that "the mere dissemination of information in the abstract was not the driver of First Amendment doctrine," but that *the content* being disclosed was itself strongly protected speech (political speech about labor unions in that case).[70] By contrast, the disclosed materials in *Defense Distributed* were computer files, whose status as protected speech was fact-dependent and in doubt according to the Third Circuit.[71]

That characterization subtly and inappropriately shifts the doctrinal focus. In *Bartnicki*, the Supreme Court clearly rejected the argument that disclosure of information is merely conduct, plainly stating that "disclosing" and "publishing" information is fundamentally speech.[72] The Court was then faced with a separate question: whether the government's interest in protecting privacy could justify liability for publishing truthful information. It held that it could not where the publisher lawfully obtained the information and the subject concerned a matter of public importance. The public or private nature of the information therefore entered the analysis only after the Court had already recognized dissemination as speech. *Bartnicki* did not treat the character of the information as a threshold question of First Amendment coverage. The Third Circuit's approach, by contrast, conditions First Amendment protection on whether the information is deemed sufficiently "expressive" rather than "functional," collapsing the distinction between recognizing speech and evaluating the permissibility of regulating it. Despite citing *Bartnicki* for this premise, the Third Circuit's reasoning has no constitutional grounding. Indeed, *Bartnicki* holds the opposite.

The Third Circuit also relied on a mischaracterization of *Sorrell*, suggesting that the Supreme Court struck down Vermont's statute *solely* on the basis that it operated as viewpoint discrimination and not because information is itself protected speech.[73] In other words, the Third Circuit asserted that *Sorrell* scrutinized the law in question only because pharmaceutical

[69] *Bartnicki*, 532 U.S. at 527.
[70] *Defense Distributed,* 971 at 507–08.
[71] *Id*. 509–10.
[72] *Bartnicki*, 532 U.S. at 527.
[73] *Id*. at 32.

marketers were subject to viewpoint discrimination, not because the underlying prescriber-identifying data was itself speech.[74]

That description is technically accurate but doctrinally incomplete. The Court in *Sorrell* began by explaining that "the creation and dissemination of information are speech within the meaning of the First Amendment" and that "[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."[75] The Court acknowledged that there was therefore "a strong argument" that the prescriber-identifying information itself was speech. The Court then stated that it need not resolve that question definitively because the statute imposed content- and speaker-based burdens on expression even *assuming arguendo*, as the State urged, that the information was merely a commodity.

The Court's argument does not weaken the proposition that information is speech; it shows the opposite. The Court assumed the State's narrower framing only to demonstrate that the statute would fail *even if* the data were treated as a mere commodity. By treating that procedural move as evidence that *Sorrell* did not recognize information as speech, the Third Circuit once again reversed the logic of the opinion.

In *Sorrell*, the Court did not engage in the sort of functionality-versus-expressiveness analysis suggested in *Corley* and relied upon by the Third Circuit in *Defense Distributed*. Again, the information at issue in *Sorrell* was highly instrumental data sold for the specific purpose of influencing physicians' prescribing behavior. Yet the Court did not ask whether the information functioned as a practical tool for real-world action. Instead, it treated the creation and dissemination of the information as speech and analyzed the statute under ordinary First Amendment principles.

Even if *Sorrell* left ambiguity at the margins, *303 Creative* did not. There, the Court held that custom wedding websites created and conveyed through software are fully protected speech. The Court emphasized that "all manner of speech" qualifies for First Amendment protection regardless of medium and reaffirmed a central First Amendment principle: the Constitution protects speech "regardless of whether the government considers [it] sensible and well intentioned or deeply 'misguided.'" The analysis did not turn on what the software executed, but on the fact that the plaintiff was being compelled to create and publish expressive content. The same principle applies in *Defense Distributed*. New Jersey plainly believes that publishing files that enable others to print firearms is harmful and misguided. But that is precisely why the First Amendment applies. The State may regulate the conduct of

[74] *Sorrell.*, 564 U.S. at 570–71.
[75] Supra note 72.

manufacturing or possessing firearms, but it may not regulate that conduct by gagging speakers who publish information about how others might act. The Constitution does not permit the government to suppress speech simply because it fears the actions that listeners might take after hearing it.

The Third Circuit's approach in *Defense Distributed* therefore rests on a doctrinal mistake. The court does not deny that some software may be speech, but it conditions First Amendment protection on a multi-factor inquiry into whether the code is sufficiently expressive rather than functional. That framework has no basis in Supreme Court precedent. The Court has repeatedly held that the creation and dissemination of information is speech, regardless of whether that information is technical, instrumental, or capable of guiding real-world conduct. When the Court has permitted regulation, it has done so only after recognizing speech and then evaluating whether competing interests justify the restriction under established First Amendment scrutiny.

Defense Distributed inverts that sequence. By treating the functionality of information as a threshold question of First Amendment coverage, the court effectively creates a new category of lesser-protected speech: information deemed too effective at producing action. The Supreme Court has consistently refused to recognize such categories absent a deeply rooted historical tradition. No such tradition exists for technical or instructional information. To the contrary, the Court's cases—from *Virginia Pharmacy* and *Bartnicki* to *Sorrell* and *303 Creative*—confirm that the publication of information remains speech even when that information enables others to act.

For that reason, the proper framework is straightforward. Publishing software is the dissemination of information and therefore speech. Regulations aimed at that publication must be evaluated under the First Amendment's ordinary rules governing prior restraints, compelled speech, and content-based restrictions. Attempts to deny coverage based on the perceived functionality of the information depart from both the structure and the history of First Amendment doctrine.

D. Application to Software Publication

Applying the Supreme Court's distinction between pure speech and expressive conduct to software publication—particularly blockchain node software, smart contracts, and user-directed intefaces—makes clear that publishing such software is pure speech rather than conduct. Publishing crypto software is the creation and dissemination of information composed of words and symbols that convey scientific knowledge and express political or societal ideas.

i. Publishing Software is a Form of Disseminating Information

In *Bartnicki* and *Sorrell*, the Court made it clear that information is entitled to First Amendment protections on its own. At its foundation, software is information set up as computer instructions that convey technical facts of how something works or how to achieve a specific outcome (if you do x, then y occurs). Even setting aside its expressive attributes, which will be discussed in the next subsection, publishing software is no different from publishing raw scientific data that allows for research or experimentation, or from publishing economic data that guides political or business discussions.

Much speech also has practical functionality, including recipes, lab protocols, blueprints, operating manuals, musical scores, mathematical formulas, and legal instruments. As explained in *Bartnicki* and *Sorrell,* the fact that information may guide others' conduct does not remove it from the protections of the First Amendment. The fact that information can sometimes require a tool, such as a computer, does not change this reality either; just like tools can be used for cooking recipes or instruments for playing music. This is the premise of instructions: speech that others may use for their own purposes, using the appropriate tools. There is a speaker and there is a conductor. And, as previously explained, the two are distinct, especially in the context of blockchain networks, smart contracts, and user-controlled interfaces.

In a blockchain network, the person operating a node uses publicly-available software to participate in a network alongside others conducting the same activity. The publisher of the software does not operate the network, but merely publishes the instructions for others to use with their computers. With smart contracts, users sign transactions with their private keys and broadcast them to network nodes. Each node independently executes the contract's bytecode on its own computer to validate the transaction and update its copy of the blockchain. The publisher or "deployer" of that contract does not execute the code. The publisher merely makes the instructions available in a place (the blockchain) where others may independently choose to run them. The same holds true for publishers of many UIs. In the case of software for purely informational and user-controlled UIs at least, the publisher is simply making computer instructions publicly available on the Internet for independent third-parties to use.

In these instances, the publisher is not participating in any capacity beyond a publisher. They merely wrote the software and made it publicly available for users to read and use to operate a given task. Furthermore, despite the Third Circuit's assertion in *Defense Distributed*, the instantaneous execution of software instructions is not relevant to the First Amendment inquiry. What matters is the distinction between publication and operation. The author of the software publishes instructions; others choose whether to run them. Therefore, even though

crypto software has the ability to be used to conduct certain activities—and thus is "functional" under *Corley* or *Defense Distributed* standards—the author of the speech and the operator of its instructions are still distinct individuals. And so, to equate writing software with conducting an activity is no different than equating publishing a cookbook with cooking a meal.

We would not deny Julia Child First Amendment protection because her recipes appear in a cookbook rather than a novel, or because she hoped readers would easily turn her words into *coq au vin*. Nor would we begrudge composer Hans Zimmer protection because he distributes his music as MIDI files rather than handwritten scores, knowing producers may instantly rearrange them on computers. And we would not strip Banksy of protection because he paints on public walls hoping to provoke protest and civil disobedience. Many of history's most influential speakers have chosen a particular medium precisely because it makes action easier. Often *the medium is the message*.[76] Denying First Amendment protection to certain media because they facilitate action is therefore little more than an attempt to suppress the particular messages best conveyed through them.

ii. Software is Pure Speech

Crypto software also qualifies as pure speech under the First Amendment because it satisfies the characteristics of protected expression recognized in *303 Creative LLC v. Elenis*. To review, in that case, the Court held that custom wedding websites constituted protected speech because they contained "images, words, symbols, and other modes of expression," that were the creator's "original, customized" work, and communicated the creator's own ideas. The Court further emphasized that the medium of expression—websites, which are software and data delivered over the Internet—does not alter the First Amendment analysis.

First, software consists entirely of words and symbols logically organized to communicate information. Whether written as human-readable source code or compiled into machine-readable bytecode or object code, the underlying structure remains linguistic and symbolic. Programmers read, interpret, critique, and modify code just as a musician reads and annotates a composer's score. Machine or object code is no different than a player piano roll.[77] Even a piano roll still depends on a human performer to load the roll and operate the instrument; the technology merely lowers the level of skill required to perform the work. The roll remains expression, even though it is designed to make execution easier. Software operates in the same way. It communicates instructions that others may choose to run, often with the aid of machines that simplify the process. Blockchain software works similarly: developers

[76] Marshall McLuhan, *Understanding Media: The Extensions of Man* 7 (1964) (introducing the concept that "the medium is the message").
[77] Van Valkenburgh, *Electronic Cash*, supra note 12.

publish instructions, while node operators and users decide whether to execute those instructions on their own machines.

Second, software development is inherently creative. Developers design protocols, algorithms, and systems through original arrangements of code. Even when building upon open-source projects, as is common in the blockchain ecosystem, new versions incorporate novel improvements, optimizations, and architectural decisions made by the developer. In this respect, software development resembles other creative disciplines such as literature, music, or film, where new works often emerge from reinterpretations and expansions of earlier ideas.

The history of Bitcoin illustrates this clearly. When Satoshi Nakamoto introduced Bitcoin in 2008–2009, he did not merely describe an idea in abstract terms. He expressed the idea through working source code. That code embodied a novel combination of cryptographic primitives, network protocols, and economic rules that together demonstrated something many experts had long believed impossible: that peer-to-peer digital money could function over the internet without trusted intermediaries. Had Nakamoto written only a theoretical essay, the idea might have remained speculative. By publishing code, however, he made the idea testable. Others could run it, study it, modify it, and verify that the system worked. In that sense, the software itself was the message.

Since that initial publication, thousands of developers have contributed their own creative work to the Bitcoin and Ethereum codebases and to countless other blockchain projects. Each contribution—whether a protocol improvement, a performance optimization, or a new smart contract—represents an original intellectual effort expressed through software. These repositories function much like collaborative scientific or artistic works, where contributors build upon one another's ideas while adding their own.

Software publication therefore represents not merely the transmission of technical instructions but the expression of human creativity and innovation. Like scientific papers, musical compositions, or architectural designs, software captures ideas in a form that others can study, interpret, and build upon. Sometimes the form of the expression is inseparable from the idea itself.

Third, publishing software is done to express scientific ideas and "facts that advance human knowledge and allow us to conduct human affairs."[78] Software specific to cryptocurrency is also published to express ideas for "political or social goals… such as individual privacy and

[78] *Id.*

agency over one's own financial dealings."[79] In fact, one could argue that most cryptocurrency software is inherently political. The concept of cryptocurrency (i.e., digital or electronic cash, electronic currency, etc.) goes back all the way to the early 1990s with the Cypherpunk[80] mailing list, where cryptographers were sharing their thoughts on a financial system based on privacy and agency over one's own financial dealings.[81] Satoshi Nakamoto, author of the Bitcoin whitepaper and software protocol, explicitly stated their ideological reasoning for publishing the software in a 2009 email:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible… It's time we had the same thing for money. With [electronic]-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless."[82]

The publication of blockchain software therefore communicates not only technical knowledge but also ideas about how financial systems should be organized. For these reasons, publishing crypto software satisfies the standard articulated in *303 Creative*. Like the wedding websites in that case, blockchain protocols, smart contracts, and user-controlled interfaces are composed of symbolic expression created by developers to communicate ideas and technical knowledge. Their publication is therefore pure speech.

At the same time, not every act performed by a crypto software developer is pure speech. A crucial distinction must be drawn between publishing software and operating systems built upon that software. Publishing code—whether in a repository, on a website, or on a blockchain—is the dissemination of information and therefore speech. Operating services, exercising control over systems, or taking custody of user assets may involve conduct subject to

---

[79] Coin Ctr., *Broker Comment*, supra note 13.
[80] Cypherpunks were a community of technologists and activists in the 1990s who believed in using cryptography to achieve individual privacy and freedom in the Information Age. Eric Hughes, *A Cypherpunk's Manifesto* (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html.
[81] marc@mit.edu, thoughts on digital cash (Cypherpunks mailing list message) (Nov. 29, 1992, 5:08 PM), *Cypherpunk Archives*, https://cypherpunk.maaria.com/.
[82] Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency* (Feb. 11, 2009, 22:27 UTC), Satoshi Nakamoto Inst., https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/.

regulation. The First Amendment does not prohibit regulation of such conduct simply because computers are involved. This section focused on publication alone. Questions concerning operation, control, or custodial authority implicate separate doctrines—particularly the distinction between protected publication and regulated professional conduct—and will be addressed later in this report.

IV. Restrictions and Compulsion

Once the publication of software is recognized as speech, the constitutional analysis becomes straightforward. The First Amendment sharply limits the government's ability to control when speech may be published, what viewpoints it may express, and what messages speakers must convey. Laws that require government approval before speech may be published operate as prior restraints. Laws that disfavor particular speakers or viewpoints trigger strict scrutiny as content- or speaker-based restrictions. And regulations that force speakers to include government-preferred messages constitute compelled speech.

These doctrines form the framework for evaluating attempts to regulate the publication of crypto software.

A. Content- and Speaker-Based Restrictions

The Supreme Court has repeatedly held that laws targeting particular speakers or viewpoints are presumptively unconstitutional. The Court's modern articulation of this principle appears most clearly in *Sorrell v. IMS Health Inc*.

To review, *Sorrell* involved a Vermont law restricting the sale and use of prescriber-identifying pharmaceutical data.[83] Pharmacies were prohibited from selling the information to pharmaceutical marketers but permitted to disclose it to other speakers, such as researchers.[84] The Court held that the law "does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers."[85] Because the statute allowed some speakers to use the information while restricting others, it imposed content- and speaker-based burdens on protected speech and therefore triggered heightened scrutiny.[86]

The Court also concluded that the law reflected viewpoint discrimination.[87] Vermont sought to suppress marketing speech using the data in order to "tilt public debate in a preferred

[83] *Sorrell*, 564 U.S. at 552.
[84] *Id.* at 559.
[85] *Id.* at 567.
[86] *Id.* at 552.
[87] *Id.* at 565.

direction."[88] That objective, the Court explained, is fundamentally incompatible with the First Amendment.[89]

Sorrell therefore confirms two principles directly relevant to software publication. First, creating and disseminating information is itself protected speech. Second, the government may not selectively burden speakers who disseminate disfavored forms of information or advocate disfavored ideas.

Crypto software *is* politically controversial and its proliferation has profound ramifications for democracy, law enforcement, personal privacy, and individual autonomy in financial dealings. It is exactly because of that controversy that the publication and dissemination of crypto software *cannot* be specifically targeted for state restrictions as compared with other types of financial software, e.g. online banking software or software with embedded government surveillance. To do so would, unequivocally, be a transparent attempt to "tilt public debate" over financial freedom and privacy "in a preferred direction" for those seeking to maintain existing systems of corporate and government financial surveillance and control. Regardless of one's opinion on crypto, any anti-crypto viewpoint discrimination is fundamentally at odds with the goals of the First Amendment, has no basis in precedent, and is unconstitutional.

B. Compelled Speech

The First Amendment not only protects the right to speak. It also protects the right *not* to speak. The Court reaffirmed this principle in *National Institute of Family & Life Advocates v. Becerra* (2018), *303 Creative LLC v. Elenis* (2023), and most recently in *Chiles v. Salazar* (2026).

In *NIFLA*, California required crisis pregnancy centers to provide government-drafted notices promoting state abortion services.[90] Because the law forced a narrow class of speakers to deliver a message they opposed,[91] the Court held that the law was an unconstitutional content-based regulation compelling speech. In *NIFLA* we also find the intersection of viewpoint discrimination and compulsion. In his concurrence, Justice Kennedy pointed out that viewpoint discrimination was "inherent in the design and structure" of the statute because California targeted pro-life clinics, forcing them to adhere to a notice requirement that

[88] *Id.* at 555.
[89] *Id.* at 565.
[90] *Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 585 U.S. 755, 760–61 (2018).
[91] *Id*. at 777.

contradicted the speaker's deeply held beliefs while promoting the government's preferred message.[92]

The Court applied the same principle in *303 Creative*. To recap, in this case Colorado sought to require a website designer to create wedding websites celebrating same-sex marriages. The Court held that the First Amendment prohibits the government from forcing speakers to create expressive content conveying messages with which they disagree. Even though the designer operated a commercial business and offered services to the public, the state could not "coopt an individual's voice for its own purposes."[93]

The Court emphasized that this protection applies even when the government believes the speaker's views are misguided or harmful. The Court explained that "First Amendment's protections do not [just] belong to speakers whose motives the government finds worthy; its protections belong to all, including to speakers whose motives others may find misinformed or offensive."[94]

The Court then reiterated these same principles in *Chiles*, where it held that when Colorado applied its conversion-therapy ban to a licensed counselor's talk therapy, the law regulated speech based on its viewpoint.[95] Using *NIFLA*, the Court found that the State compelled its favored speech when it only allowed for counseling that affirmed one direction of identity development while it forbid counseling aimed at another,[96] and again solidified that "the First Amendment protects the inalienable right of every individual to decide for himself 'how best to speak'"[97] and that "no official…may command our tongues or silence our voices."[98]

Importantly, in certain cases, regulators may argue that disclosure mandates do not raise serious First Amendment concerns because they merely compel the communication of factual information. The Supreme Court has acknowledged that narrow disclosure requirements involving "purely factual and uncontroversial information"[99] may sometimes be permissible, particularly in the context of commercial advertising or other regulated activities where the speaker already possesses the relevant information. In such circumstances, the compelled speech is treated as incidental to the regulation of underlying conduct.

---

[92] *Id*.
[93] *Id*. at 593.
[94] *Id*.
[95] *Chiles v. Salazar*, No. 24-539, slip op. (U.S. Mar. 31, 2026), https://www.supremecourt.gov/opinions/25pdf/24-539_fd9g.pdf.
[96] Pg. 17
[97] Pg. 8, also citing *Riley v. National Federation of Blind of N. C., Inc.*
[98] Pg. 8 citing *West Virginia Bd. of Ed. v. Barnette*, 319 U. S. 624, 642 (1943).
[99] *Zauderer v. Off. of Disciplinary Couns.*, 471 U.S. 626, 651 (1985).

But the Court has repeatedly emphasized that this doctrine is limited. In *NIFLA*, the Court rejected attempts to expand the factual disclosure doctrine beyond its narrow context, explaining that compelled factual disclosures are permissible only where the government requires the disclosure of purely factual, uncontroversial information about the speaker's own goods or services, and where the mandate does not compel the creation of new expression or otherwise impose an undue burden on the speaker's message.[100] Additionally, in *Chiles,* the Court invoked *NIFLA*'s rejection of a distinct "professional speech" category, holding that even where the government may require limited factual disclosures ancillary to otherwise regulable conduct, it may not use licensing or registration to force speakers to carry the State's preferred message and enforce conformity (more on speech and professional conduct in the next section).[101] Outside those narrow contexts, laws that compel speech remain subject to heightened First Amendment scrutiny.

Most importantly, the factual disclosure doctrine applies only where the compelled speaker already possesses the information being disclosed and where the disclosure requirement is incidental to the regulation of an underlying professional or commercial activity. When the government instead compels speakers to generate new information, redesign their communications, or create new expressive works in order to satisfy a disclosure mandate,

[100] *See, e.g., Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626, 651 (1985) (permitting disclosure requirements limited to "purely factual and uncontroversial information" in attorney advertising); *Milavetz, Gallop & Milavetz, P.A. v. United States*, 559 U.S. 229, 250 (2010) (upholding disclosure requirements that "accurately describe the advertised services"); *Nat'l Inst. of Family & Life Advocates v. Becerra*, 585 U.S. 755, 766–68 (2018) (rejecting expansion of the doctrine and emphasizing that compelled factual disclosures are permissible only in limited circumstances); *Am. Beverage Ass'n v. City & Cnty. of San Francisco*, 916 F.3d 749, 756–58 (9th Cir. 2019) (en banc) (invalidating a compelled warning that unduly burdened the speaker's message); *303 Creative LLC v. Elenis*, 600 U.S. 570, 589–91 (2023) (distinguishing permissible factual disclosures from compelled creation of expressive content).
[101] *Chiles* at pgs 20-23.

the regulation no longer resembles a simple reporting requirement.[102] It becomes a direct compulsion of speech.[103]

For that reason, the question in compelled speech cases is not merely whether the government demands the communication of facts. It is also whether the government is forcing a speaker to express and convey a message the speaker would not otherwise express. When that occurs, the First Amendment's prohibition on compelled speech applies in full. As we will discuss in greater detail later, rules that require developers to fundamentally rewrite their software in ways that diverge from their beliefs and goals, e.g. to include government backdoors or collect and report government sought information, should be understood as unconstitutional viewpoint- and content-discriminatory compulsions.

Together, these cases establish a simple rule: the government may not force speakers to include government-preferred messages in their speech.

C. Prior Restraints

Licensing regimes that condition the publication of speech on prior government approval raise an additional First Amendment concern: prior restraint. The Supreme Court has long treated systems that require speakers to obtain permission before speaking as among the most constitutionally suspect forms of regulation.

In *Near v. Minnesota*, the Court explained that the central purpose of the First Amendment was to prevent government regulations that suppress speech before publication.[104] The Court reaffirmed this principle in *Lovell v. City of Griffin*, striking down an ordinance that required individuals to obtain government permission before distributing literature. The Court held that conditioning publication on prior approval places officials in the position of deciding

---

[102] *See Nat'l Inst. of Family & Life Advocates v. Becerra*, 585 U.S. 755, 766–68 (2018) (rejecting compelled notices that were not limited to factual disclosures about the speaker's own services); *Am. Beverage Ass'n v. City & Cnty. of San Francisco*, 916 F.3d 749, 756–58 (9th Cir. 2019) (en banc) (invalidating disclosure requirements that unduly burdened the speaker's message).

[103] *See Wooley v. Maynard*, 430 U.S. 705, 714 (1977) (holding that the First Amendment protects the right not to be compelled to "use their private property as a 'mobile billboard' for the State's ideological message"); *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.*, 515 U.S. 557, 573 (1995) (government may not require speakers to alter the expressive content of their message); *303 Creative LLC v. Elenis*, 600 U.S. 570, 588–91 (2023) (holding that the state cannot compel a speaker to create expressive content conveying a message the speaker does not wish to convey).

[104] *Near v. Minnesota*, 283 U.S. 697 (1931).

who may speak and what may be said, which is precisely the form of censorship the First Amendment was designed to prevent.[105]

For that reason, the Court has consistently treated licensing regimes affecting speech with deep skepticism and permitted them only under narrow circumstances with strict procedural safeguards. A regulatory system requiring developers to obtain licenses or approvals before publishing software would give reason for this skepticism. Such a regime would give regulators advanced control over who may publish code and what features that code must contain, an arrangement the Courts have long treated as incompatible with our First Amendment freedom of speech.

These principles have direct implications for the regulation of crypto software. When the government conditions software publication on compliance with licensing regimes designed for financial intermediaries, it risks transforming protected speech into regulated activity. The constitutional question is not whether financial services may be regulated—they plainly may—but whether the government may regulate those services by controlling who is permitted to publish the software that enables them. As the following section explains, several recent regulatory proposals and prosecutions raise precisely that concern.

D. Application to Software Publication

In recent years, publishers of crypto software have increasingly faced legislative proposals, regulatory rulemakings, and criminal prosecutions that risk treating the publication of software as the regulated operation of financial services. Several prominent examples illustrate the problem.[106]

The Securities and Exchange Commission has proposed and then withdrawn rules that would expand the definition of "exchange" in ways that could encompass developers who merely publish software enabling peer-to-peer trading of digital assets.[107] Similarly, in 2023, the

---

[105] *Lovell v. City of Griffin*, 303 U.S. 444 (1938).

[106] *Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales*, 89 Fed. Reg. 106,928 (Dec. 30, 2024) (to be codified at 26 C.F.R. pt. 1); *Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of "Exchange"*, 88 Fed. Reg. 29,448 (proposed May 5, 2023) (to be codified at 17 C.F.R. pts. 232, 240, 242 & 249).

[107] Peter Van Valkenburgh, Coin Ctr., *Comments to the Securities and Exchange Commission on Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems* 2–3 (Apr. 14, 2022), https://www.coincenter.org/app/uploads/2022/04/SEC-Exchange-Rule-Comment.pdf; Peter Van Valkenburgh, Coin Ctr., *Further Comments to the Securities and Exchange Commission on Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems* 6 (June 7, 2023), https://www.coincenter.org/app/uploads/2023/06/Coin-Center-Second-Comment-re-S7%E2%80%9302%E2%80%9322.pdf.

IRS finalized a rule expanding the statutory definition of "broker" to potentially include persons who publish cryptocurrency software tools or websites. That rule would have imposed extensive reporting obligations on these publishers even though they neither control user assets nor maintain customer relationships.[108] Congress later repealed the rule through a joint resolution under the Congressional Review Act.[109]

In the more extreme cases, criminal enforcement actions have blurred the line between software publication and financial operation, even in spite of contradictory law and regulatory guidance.[110] In 2023, the DOJ indicted Roman Storm, a developer associated with the Tornado Cash protocol, charging him with conspiracy to operate an unlicensed money transmitting business, [111] conspiracy to launder money, and conspiracy to violate sanctions laws.[112] The indictment repeatedly cited the absence of user identification mechanisms—commonly referred to as "know-your-customer" or KYC procedures—as evidence of unlawful conduct.[113] In effect, the prosecution treated Storm's decision to publish software that allowed users to transact privately as evidence that he had failed to design his software in accordance with government preferences.[114]

Although these actions arise in different legal contexts, they share a common premise: that software publishers may be required to design and publish their software so that they conform to government-approved financial architecture. Under this premise, software that allows users to transact independently, without intermediaries or identity verification, may be treated as unlawful unless it is redesigned to incorporate surveillance or intermediation features.

That premise raises serious First Amendment concerns. At bottom, these regulatory approaches do not merely regulate financial conduct. They attempt to control the content and design of software publications. In practical terms, the government's position implies two preferred viewpoints about how cryptocurrency systems should function. First, that crypto transactions should occur through identifiable financial intermediaries. Second, that any

---

[108] Coin Ctr., Broker Comment, supra note 13, at 9.
[109] H.J. Res. 25, 119th Cong., 1st Sess. (Feb. 28, 2025) (as reported in House).
[110] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FinCEN Guidance FIN-2019-G001 (May 9, 2019).
[111] For an alleged conspiracy to violate 18 USC 1960. Id. at 32-34.
[112] For an alleged conspiracy to violate the International Economic Emergency Powers Act (IEEPA). Id. at 34-35.
[113] Id. at 15-20.
[114] Brief of Amicus Curiae Coin Center in Support of Defendant Roman Storm's Motion to Dismiss at 18, *United States v. Storm*, No. 23 Cr. 430 (KPF) (S.D.N.Y. filed Apr. 5, 2024), https://www.coincenter.org/app/uploads/2024/04/Coin-Center-Amicus-Brief-filed.pdf.

software published that could be facilitating those transactions should incorporate mechanisms for collecting and reporting user identity information.

Developers who publish cryptocurrency software frequently hold the opposite view. Many publish tools precisely because they believe financial infrastructure should allow individuals to transact without intermediaries and mandatory identity disclosure. Many prominent researchers and developers in this ecosystem are, in fact, chiefly motivated by the conviction that privacy and agency over one's own financial dealings is essential to the preservation of a free and open society.[115]

These views are not incidental to the software. They are expressed through the architecture of the systems developers choose to design and publish. Moreover, the regulatory proposals and enforcement actions that threaten these views are not simply economic regulations or safety requirements. Requiring the operator of a steam engine to install a governor valve to prevent explosions regulates how a machine is used. What regulators propose here is fundamentally different. It would be as if James Watt had been told he could not publish an engineering schematic for a steam engine unless it included a specific government-approved valve design—or, in some cases, that he could not publish steam engine designs at all and should instead restrict himself to improving horse-drawn carriages. The First Amendment does not permit the government to dictate the content of technical publications in this way.

First, these regulations impose content- and speaker-based restrictions on protected expression. As in the statute struck down in *Sorrell*, the government targets a particular class of speakers—developers, researchers, and publishers of crypto software—and restricts their ability to create and disseminate information based on the viewpoint that information conveys. In *Sorrell*, the Court explained that such laws are constitutionally suspect because they seek to burden speech "in order to tilt public debate in a preferred direction."[116] The same concern arises here. Developers who publish software enabling individuals to transact privately and without intermediaries express a view about the design of financial systems. Regulations that prohibit or penalize the publication of such software unless it incorporates surveillance or intermediary control mechanisms effectively suppress that viewpoint in favor of the government's preferred alternative: a financial system structured around identifiable

---

[115] Coin Ctr., *Broker Comment*, supra note 13, at 22; Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, supra note 48; marc@mit.edu, *thoughts on digital cash*, supra note 47; Hughes, *A Cypherpunk's Manifesto*, supra note 46; Jerry Brito, *The Case for Electronic Cash 1.0: Why Private Peer-to-Peer Payments Are Essential to an Open Society* (Coin Ctr. Feb. 2019), https://www.coincenter.org/app/uploads/2020/05/the-case-for-electronic-cash-coin-center.pdf.
[116] *Sorrell*, 564 U.S. at 555.

intermediaries and the mass warrantless government surveillance that is achieved via those intermediaries.

Second, these regulations do not merely burden disfavored viewpoints; they compel speakers to adopt the government's preferred one. As the Supreme Court has repeatedly emphasized, the First Amendment prohibits laws that force individuals to create expression conveying messages they do not wish to convey. In *NIFLA* and *303 Creative*, the Court rejected regulatory schemes that required speakers to produce expressive content promoting government-mandated messages. The same principle applies here. Requirements that developers design software to collect user identities, monitor transactions, or insert intermediary control points compel them to publish code embodying the government's preferred vision of financial architecture—one premised on surveillance and institutional intermediation.

These mandates therefore do more than regulate financial conduct. They compel developers to create and publish expressive software that embodies the government's preferred vision of how financial systems should operate—one built around identifiable intermediaries and routine financial surveillance. In this respect, the regulations function much like the law struck down in *Sorrell v. IMS Health*, which the Court invalidated because it manipulated the architecture of speech in order to favor certain messages and speakers over others.

For these reasons, when developers publish cryptocurrency software that others may use, they are engaged in the dissemination of information and ideas about how digital financial systems can be designed. That activity falls within the protection the First Amendment affords to the publication of technical, scientific, and political expression. At the same time, it is important to recognize that the broader ecosystem surrounding such software can involve activities that go beyond publication alone. The government may regulate the conduct of financial intermediaries who act as agents, custodians, or counterparties in transactions, and some actors in crypto systems may perform functions that resemble those traditional roles.

Accordingly, the constitutional analysis cannot end with the recognition that software publication is speech. Regulators often attempt to characterize developer activities as part of a regulated financial profession. The critical question, therefore, is where the line should be drawn between protected publication and regulable professional conduct. The next section addresses that question and explains how courts should distinguish between the two.

V. Speech and Professional Conduct

Software publication is speech, but that analysis alone does not answer every constitutional question in this report. A developer may publish software and still, through other activities, enter into a line of work that the government has long regulated: acting as an agent, custodian, adviser, or counterparty in the affairs of another. The difficulty facing regulators and courts is therefore to identify where software publication ends and regulable professional conduct begins.

A. Governing Law

Before we look at how the Court has drawn the line between speech and professional conduct, we need to flag an incorrect approach. Courts and regulators cannot treat "professional speech" as a freestanding category of lesser-protected expression. The Supreme Court has foreclosed that approach. In *NIFLA*, the Court held that it has never "recognized 'professional speech' as a separate category of speech" and that speech does not lose constitutional protection "merely because it is uttered by 'professionals.'"[117] This was further solidified in *Chiles* when the Court turned to *NIFLA* and stressed that licensing addresses qualifications for practicing a certain profession, not a professional's point of view.[118] Both of these holdings are of particular importance to crypto because most, if not all, crypto software is used to do things that once required a financial professional. What are we therefore to think about the crypto developer whose software replaced those professionals? The speaker works in finance. The software is used in transactions. The speaker is earning per-transaction fees. From these facts, regulators may hastily assume that the crypto software must inherently be less constitutionally protected than, say, art, literature, or journalism. *NIFLA* and *Chiles* rule that out; there is no free-floating "professional speech" exception waiting to be invoked whenever useful or commercially valuable expression appears near a regulated market.

That does not, however, mean that every law touching professionals is constitutionally suspect. *NIFLA* identified two narrow settings in which speech associated with professional activity may receive less protection: compelled disclosure of "purely factual and uncontroversial information" in limited circumstances, and regulation of professional conduct that only incidentally burdens speech.[119] These are not examples of lesser protected "professional speech." They are ordinary First Amendment doctrines applied to conduct that happens to occur in professional settings. This distinction means the government cannot escape full First Amendment scrutiny simply by attaching the word "professional" to the target

[117] *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371–72 (2018).
[118] *Chiles*, pg 20.
[119] Id. at 2372.

of its regulation. If the law is directed at the creation, content, architecture, or dissemination of expression, the First Amendment still applies with full force.

If, by contrast, the law is directed at conduct and burdens speech only incidentally, it may survive constitutional scrutiny. This is the holding in *United States v. O'Brien*. Where "speech" and "nonspeech" elements are combined in the same course of conduct, the government may sometimes regulate the nonspeech element even though some burden on expression results. But the burden must truly be incidental. The state's interest must be directed at a nonexpressive act with independent legal significance, not at the message, the publication, or the design of the expression itself.[120]

That incidental-burden inquiry is easy to state and easy to abuse. Regulators will nearly always say that they are not targeting speech but some surrounding business activity. Yet every modern speaker has surrounding business activity. Newspapers sell subscriptions and maintain websites. Financial data brokers sell terminals. Software developers charge license fees, maintain servers, and deploy updates. Even "influencers" get paid (if they are any good). If a revenue model or server hosting arrangement were sufficient grounds to license and police speakers, then the First Amendment would mean very little in the digital age. The *O'Brien* test is more specific: what conduct is the law using as the trigger for the duty, and what would the speaker have to do to comply? A burden is easier to characterize as incidental where the legal duty attaches to a genuinely nonexpressive role with independent legal effect, and where compliance merely requires disclosing or recording facts already obtained in the ordinary course of that role. It is much harder to characterize as incidental where the law gets its leverage only by forcing a speaker to redesign a product, collect new information, alter the architecture of a publication, or convert a self-help tool into an intermediated service.

Traditional examples make the distinction clearer. A doctor writing a prescription is not merely expressing an opinion; the doctor has assumed a legal duty to care for his patient, the prescription is speech but it also authorizes access to a controlled substance and thus has legal effect. A lawyer signing a settlement or filing a document that alters legal rights is not merely speaking; he is acting on behalf of his client and that act will bind his client in a court of law. A broker acting as agent or principal in a sale is not merely conveying market information; the broker makes a transaction with legal and financial consequences for the customer. But for the broker's fidelity to her client's interests, the client would not have the benefit of the deal she expected. In those cases, the law is not regulating publications (e.g. prescriptions, settlements, purchase orders); it is regulating an independently significant role performed by a human who

[120] *United States v. O'Brien*, 391 U.S. 367, 376–77 (1968).

is exercising judgement, and the accompanying burden on speech caused by licensing that professional or seeking certain factual disclosures from that professional is plausibly incidental.

The same cannot be said of a general publication, a widely available website, a public data dashboard, an open-source software client, a smart contract deployed for all to use, or an interface that automatically recombines public information into a more useful form. In those cases there may be speech, there may be usefulness, there may be profit, and there may be a sophisticated technological setting. But there is no separately identifiable, legally operative act of taking another person's affairs in hand unless some additional role is present. Calling the publication "conduct" does not make it so.

The Supreme Court's clearest articulation of that boundary in the financial-information context remains *Lowe v. SEC* (1985). There the government attempted to apply the licensing requirements of the Investment Advisers Act to the publisher of a general investment newsletter. The Court rejected that application. The statute, properly understood, reached the conduct of those engaged in the investment-advisory profession, not the publication of impersonal financial commentary to the public at large, even for a fee. The Court explained that the Act's "central purpose" did not encompass communications that "do not offer individualized advice attuned to any specific portfolio or to any client's particular needs" but instead "circulate for sale to the public at large in a free, open market."[121]

Justice White's concurrence in *Lowe* stated the constitutional principle more directly, and it remains the best formulation of the line between professional conduct and speech. A professional, he wrote, is one who "takes the affairs of a client personally in hand and purports to exercise judgment on behalf of the client in the light of the client's individual needs and circumstances."[122] Where that "personal nexus" does not exist, regulation "ceases to function as legitimate regulation of professional practice with only incidental impact on speech; it becomes regulation of speaking or publishing as such."[123] That is the distinction that governs here. It is not the distinction between financial speech and nonfinancial speech, nor the distinction between useful speech and useless speech. It is the distinction between general publication and delegated judgment within a client relationship.

That formulation also explains why software's high degree of usefulness, sophistication, or profitability is not enough to take it from the realm of protected speech. A general investment newsletter may be highly influential. A Bloomberg terminal may use sophisticated

[121] *Lowe v. SEC*, 472 U.S. 181, 207–10 (1985).
[122] *Id.* at 232 (White, J., concurring in the result).
[123] *Id.*

data and software to make the decision to buy or sell extraordinarily easy, fast, and well-informed. Both may be highly lucrative lines of business for their publishers. Both are valuable information products upon which investors may rely, even to their detriment. But neither thereby becomes an investment adviser or broker. In each case, the speaker provides information and tools to the public; the user remains responsible for the ultimate choice. The fact that publication is effective enough to matter does not diminish its constitutional status. It is still speech, not conduct.

More recent caselaw confirms that this line does not disappear when the publication becomes more technical, more dynamic, or more immediately useful to financial decisionmaking. In *Taucher v. Born* (1999), the government sought to require the publishers of commodities newsletters, websites, and trading software to register as commodity trading advisers. The district court rejected that effort. What mattered was not that the publications were sophisticated, or that they generated actionable recommendations, or that traders might rely on them to make rapid decisions in real markets. What mattered was that the publishers were not engaged in person-to-person advisory relationships and were not exercising judgment on behalf of particular clients. They were addressing the public at large. Their publications, including their software, therefore remained on the speech side of the line rather than the professional conduct side.[124] The same distinction has been applied in subsequent cases, which continue to treat impersonal, publicly disseminated financial publications as outside the scope of advisory regulation absent a client-specific relationship.[125]

These cases help clarify what is actually doing the work in the professional-conduct analysis. Traditional professional regulation often attaches where a legally cognizable intermediary role gives a speaker's words operative effect.[126] A broker does not merely speak; the broker's acceptance or execution of an order effects a transaction for a customer as agent or

---

[124] *Taucher v. Born*, 53 F. Supp. 2d 464, 478–84 (D.D.C. 1999). Although Taucher is only a district court decision, it remains unusually instructive because it applies *Lowe*'s publication-versus-advisory-practice distinction to the modern context of newsletters, websites, and trading software. The court held that the Commodity Exchange Act could not constitutionally be applied to publishers of generalized commodities information and software where the publishers were not engaged in person-to-person advisory relationships and were not exercising judgment on behalf of particular clients.

[125] *Commodity Trend Serv., Inc. v. CFTC*, 233 F.3d 981, 992–94 (7th Cir. 2000).

[126] See Robert Kry, The "Watchman for Truth": Professional Licensing and the First Amendment, 23 Seattle U. L. Rev. 885, 906–18 (2000); Robert Kry's synthesis of these cases remains useful, particularly his emphasis on the distinction between generalized publication and person-to-person, client-specific advisory relationships. Because his article predates *National Institute of Family & Life Advocates v. Becerra*, however, it should not be read to preserve any freestanding category of lesser-protected "professional speech," which *Becerra* expressly rejected. It remains valuable as an account of the *Lowe* line and of the conditions under which regulation targets genuine professional conduct rather than "speaking or publishing as such."

principal. A lawyer does not merely communicate; the lawyer files an instrument, settles a matter, or otherwise acts within a recognized legal role that changes a client's position. A bank or custodian does not merely publish account information; it holds assets and executes instructions from a position of institutional control. In each case, the regulated actor occupies a role in which the legal system or a commercial contractual arrangement gives the actor's words or actions operative significance in the affairs of another. Merely automating aspects of these financial services would not change the first amendment analysis. A bank could not claim it doesn't owe a customer FDIC insurance because they opened the account via the bank website rather than in a branch office. The reason is not because professional speech (the bank's website) gets less protection, it's because the bank is engaged in legally binding professional conduct on their behalf whether it does so with a handshake or an "http://etc."

Blockchains are different in a way that matters here. They can remove the need for intermediary roles altogether by allowing users to make operative commitments for themselves through software that will execute irrespective of any third party. A user signs a transaction, broadcasts it, and, if it satisfies the protocol's rules, the network processes it. The operative effect no longer depends on a broker taking the order, a bank honoring the instruction, or some other intermediary occupying a legally cognizable role between the speaker and the outcome. The protocol and the consensus system perform that function instead. That shift is not incidental to the analysis here. It helps explain why many crypto tools look less like regulated professional services and more like the publication of user-facing instruments through which individuals may act for themselves.

None of this means that blockchain systems eliminate agency relationships or professional conduct altogether. Many users will still prefer custodians rather than managing their own cryptographic keys. Many will still prefer tailored investment advice rather than generalized information, analytics, or maps of on-chain liquidity. And many firms will continue to occupy those traditional intermediary roles. Ordinary professional regulation remains available for situations where an actor truly acts as a custodian, agent, principal, adviser, or other fiduciary intermediary. The point is narrower but more important. Where users act for themselves through published software and protocol rules, the law should not pretend that a professional intermediary has taken their affairs in hand when none has. The continued existence of genuine intermediaries is no reason to reclassify self-help tools and public software as if they were the same thing.

Together, *NIFLA, Chiles, O'Brien, Lowe, Taucher*, and *Commodity Trend* establish the governing rule for the rest of this section. There is no separate category of less-protected "professional speech." The government may regulate actual professional conduct and may

incidentally burden speech in doing so. But in the information and software context, that line is crossed only when the speaker ceases to be a publisher addressing the public and instead assumes a role of agency, custody, delegated judgment, or ongoing discretionary control over the affairs of another.[127]

B. Application to Software Development

As we reviewed in the previous sections, the *sine qua non* of First Amendment protection for software is not whether the software is useful, profitable, interactive, or capable of facilitating activity that the government may regulate elsewhere. Nor is the key question whether the developer operates a business, maintains servers, deploys updates, or earns fees from usage. Those facts describe nearly every modern publisher. The question is whether the developer or operator has crossed the line from publication and its associated conduct (web design, server maintenance, etc.) into a trusted client-focused role, like agency, custody, delegated judgment, or discretionary control over the affairs of another.

That inquiry must proceed category by category. "Crypto software" is not one thing. A permissionless node client is not a hosted trading interface. An immutable smart contract is not a continuously upgradeable vault whose strategy changes whenever its publisher pushes new logic. A wallet that lets a user sign and broadcast her own transaction is not the same as a backend service that can steer, refuse, or materially alter the user's path to execution. The law should not flatten these differences. But neither should technical complexity obscure the basic point. Publication remains publication unless and until the developer begins, in a legally meaningful sense, to take the user's affairs in hand.

i. Node Clients

A permissionless node client is the simplest case. A developer writes software implementing a blockchain protocol and publishes it to the world. Others independently decide whether to download it, compile it, modify it, and run it on their own machines. The developer does not thereby operate those nodes, direct those users' transactions, or assume responsibility for their affairs. The software may be indispensable to the functioning of the network. It may embody technical and political commitments about openness, censorship resistance, or financial autonomy. None of that transforms the act of publication into professional conduct. It

[127] *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371–72 (2018); *United States v. O'Brien*, 391 U.S. 367, 376–77 (1968); *Lowe v. SEC*, 472 U.S. 181, 207–10, 232 (1985) (White, J., concurring in the judgment); *Taucher v. Born*, 53 F. Supp. 2d 464, 478–84 (D.D.C. 1999); *Commodity Trend Serv., Inc. v. CFTC*, 233 F.3d 981, 992–94 (7th Cir. 2000).

remains, in *Lowe*'s terms, a communication to the public at large, not delegated judgment for a particular client.

This remains true even though the software is highly "functional." The Constitution does not withdraw protection from a publication because it is effective, widely adopted, or central to an infrastructure of public importance. If anything, those features make prior restraint *more* dangerous, not less. A node client is still a publication even if thousands of people choose to rely on it.

The harder case is a permissioned network. There, the same actor who publishes the software may also decide who is allowed to participate as a node, who may validate, who may propose blocks, or who may otherwise join the operational network. Those additional activities may matter a great deal for statutory purposes. They may also matter for constitutional purposes. A person who identifies participants, grants or denies access, and maintains a gatekeeping role may well be doing more than publishing code.

But the correct course is to separate those roles rather than collapse them. Publishing the node software remains speech. Additional conduct may also exist: operating a gated network may mean legally identifying participants and administering their access. Those activities may, depending on their specifics, be regulable. These activities do not, however, retroactively transform the publication of the software into professional conduct. The existence of conduct alongside speech does not abolish the distinction between them.

The same point applies to backwards-compatible updates. Publishing a new release is still publishing. Recommending that users adopt a bug fix or performance improvement is still just recommending. The user remains free to run the old client, switch to another client, fork the code, or opt out entirely. The developer has not taken the user's affairs in hand simply because the developer continues to speak.

ii. Smart Contracts

Smart contracts are similarly not simply one thing. At one end of the spectrum lies the straightforward case: a developer writes a contract, compiles it, and deploys it to a public blockchain where it is available for anyone to use. Users decide whether to interact with it. Nodes execute it according to the protocol rules. The developer does not thereby take any user's affairs in hand. The contract may automate a swap, issue a token, manage collateral, or implement a strategy. But absent anything else, the developer's role remains the publication of a rule set for general use. This is not fundamentally different from publishing a form contract, like the International Swaps and Derivatives Association's (ISDA) Master agreement for commodity swaps, and it should be no less constitutionally protected from prior restraint.

That remains true even where the software embodies a sophisticated financial strategy. Take, for example, non-custodial "vault" smart contracts,[128] lending tools, and automated market makers ("AMMs"). A vault that rebalances user assets deterministically according to a published algorithm, a lending protocol that enforces collateral ratios automatically, or an automated market maker that follows a predefined formula to price and facilitate swaps may all be highly consequential pieces of financial software. That does not by itself make their developers into advisers, brokers, or fiduciaries. The code may be useful. It may automate activity that once required a human intermediary. But the relevant question is not whether the software substitutes for some function once performed by a professional. The question is whether the developer has retained a role in which the developer exercises judgment on behalf of a particular user. Where the user chooses whether to deposit, withdraw, interact, or abstain, and where the contract executes according to publicly knowable rules, the developer remains a publisher.

The harder cases begin when the developer retains powers after deployment. Admin keys, proxy patterns, upgrade rights, pausing authority, fee switches, blacklisting functions, oracle controls, and similar mechanisms do not automatically erase the speech character of publication. But they may indicate that the developer is doing more than publishing a static tool. The right analysis is not whether the contract is "functional." The right analysis is whether the developer has retained the ability to substitute the developer's later judgment for the user's earlier choice.

Once again, let's take non-custodial vaults as an example.[129] A static and immutable vault strategy contract chosen by a user at deposit is strongest for the publication side. The developer has published a strategy; the user has adopted it. If the developer later devises a better strategy and publishes that too, and the user affirmatively chooses to move to the new one, the case remains much the same. The new strategy is simply a new publication. Even a visible in-product prompt asking whether the user wants to upgrade remains close to the publication side of the line, because the user is still making the operative choice regarding their affairs and the best interests.

---

[128] A crypto vault smart contract is a non-custodial smart contract into which a user deposits tokens while retaining an on-chain claim, via a receipt token, on the user's proportional share of the vault; the contract, rather than a human intermediary, deploys the pooled assets according to predefined strategies, and the user later redeems against the contract for the underlying assets plus or minus performance. Yearn's docs describe vaults as "contracts on the Ethereum blockchain" into which users "deposit cryptocurrency tokens," receive a "receipt token," and have those pooled assets directed by the vault's "Strategies," which underscores the key point here: the assets are governed by the contract's rules rather than held by a traditional custodian.

[129] Thank you to Lewis Cohen, co-chair and partner at CahillNXT, for sharing this example in conversation with the authors.

The first genuinely difficult case is where a default upgrade to the vault strategy occurs *unless* the user affirmatively declines. There, the developer's changing judgment begins to alter the user's financial posture absent fresh assent. At that point, the relationship becomes harder to characterize as mere publication, not because the code is any less expressive than before, but because the developer's later decisions have begun to matter in an ongoing way for the user's live position.

And at the far end of the spectrum lies a continuously auto-updating vault or strategy manager: software that changes whenever the publisher pushes new strategy logic or new parameters, such that the user's funds remain subject in practical terms to the developer's evolving judgment unless the user exits entirely. That is the strongest case for professional-conduct treatment rather than simple speech protections. The developer there begins to look less like a publisher of tools and more like a manager of an ongoing financial strategy for users. Regulating that manager's conduct and their duties to their users should withstand constitutional scrutiny so long as the burden on their speech is incidental.

The same analysis applies to admin keys and proxy contracts more broadly. Narrow powers to fix bugs, preserve compatibility, or make bounded and disclosed maintenance changes do not necessarily amount to taking another's affairs in hand. Design features that preserve meaningful exit, such as withdrawal rights, opt-outs, or "rage quit" mechanisms, reinforce that conclusion because they allow the user to protect herself without depending on the developer's ongoing intervention. But *unilateral* powers to redirect value, alter material economic terms, freeze positions, seize or reroute assets, or continuously reconfigure a user's financial exposure may do so. The constitutional issue is not that the contract "does things." Many publications help people do things. The issue is that the developer may have retained a continuing role in which the developer's judgment, rather than the user's own choices, governs the user's affairs.

This is also the point where blockchain's disintermediating structure matters most. Traditional professional regulation often attaches where a legally cognizable intermediary role gives a speaker's words operative effect. A broker's acceptance of an order effects a transaction for a customer as agent or principal. A lawyer's filing binds a client or changes a legal position. A bank executes an instruction from a position of institutional control and chartered obligation. Smart contracts often remove the need for such intermediary roles altogether. A user signs and submits an instruction, and, if it satisfies the protocol's rules, the network executes it, mindlessly and reliably. The operative effect does not depend on a broker taking the order, a bank honoring the instruction, or some other intermediary occupying a legally cognizable role between the speaker and the outcome. The protocol does that work. That shift does not eliminate professional conduct altogether, but it does explain why the mere

publication of self-executing financial software cannot simply be assumed to be the modern equivalent of intermediary practice.

Nor is blockchain disintermediation some unprecedented legal anomaly. People have always been able to transact without agents, brokers, or other intermediaries where ownership and transfer were mediated by technical or practical systems rather than by account-based legal relationships: face-to-face exchanges of cash, goods, or bearer instruments are familiar examples. The law never responded to those forms of direct exchange by reclassifying the makers of paper, the printers of certificates, or the publishers of market information as brokers or custodians. That would have been absurd. Blockchain systems are novel technologies that recreate ancient capabilities. They allow people to act for themselves through a technical system of transfer rather than through a legally cognizable intermediary role. The mere fact that software facilitates such self-help does not justify treating its publisher as the absent intermediary.

iii. User Interfaces

User interfaces require the most care because they range from pure publication to full, trusted intermediation, often within products that look similar to ordinary users. The governing principle remains the same. The law should not ask whether the interface is particularly useful, intuitive, or whether it sits close to financial action. It should ask what role the operator actually plays in the user's affairs.

A purely informational interface sits comfortably on the publication side. A dashboard that displays balances, trades, governance settings, pool compositions, contract data, or other on-chain information in a more readable or condensed form is no more a financial professional than a market newsletter, a ticker screen, or a data terminal. It may influence behavior. It may be indispensable to understanding the system. But it remains the repackaging and presentation of information to the public.

User-controlled wallets and front ends ordinarily remain on the publication side as well, even where they are more interactive. These tools may 'know' what assets a user has, accept a user's desire to swap one asset for another, scan on-chain liquidity, estimate slippage, construct transaction data, and present routes. Those are meaningful functions. But they do not, by themselves, amount to taking the user's affairs in hand. They are reactive computations and tool-like outputs that programmatically respond to users' requests, not delegated judgment within a fiduciary relationship. Many developers deliberately build these interfaces so that it is impossible, or nearly so, for the publisher or maintainer to know how particular users are employing the software. And modern technical design can preserve that distance even where the developer hosts the tool on proprietary infrastructure, just as end-to-end encrypted

messaging can leave even the service provider unable to read the contents of user communications. That fact alone should not be dispositive. A developer does not become a professional intermediary merely because the software is imperfectly privacy-preserving or because the operator *could* observe some user activity. But where the developer cannot even meaningfully glean a user's affairs, the case for treating the relationship as impersonal publication rather than agency, custody, or other traditional professional conduct becomes especially strong.

This is where the Bloomberg terminal is a useful modern illustration. Bloomberg uses sophisticated software and immense data resources to make the ultimate decision to buy or sell fast and easy. It may even feel, from the user's perspective, as though the terminal is doing a great deal of the decisionmaking work. Yet no one thinks Bloomberg thereby becomes a broker or investment adviser merely by running their terminal business.[130] The user still chooses. The terminal does not owe fiduciary duties to the user. It does not bind the user to a transaction. It does not take the user's affairs personally in hand. The same should ordinarily be true of software that automatically matches user-provided information with on-chain information in order to generate prices, routes, liquidity maps, slippage estimates, or transaction drafts. The software may be extraordinarily effective. That does not change its constitutional character.

Traditional intermediary regulation is often justified by information asymmetries and agency costs: the customer cannot easily observe what the broker knows, how the intermediary routes orders, whether the adviser is conflicted, or whether the service provider is faithfully executing the customer's instructions. Many crypto interfaces and open-source routing tools reduce rather than increase those asymmetries. Protocol rules, balances, liquidity positions, transaction history, and available on-chain paths may all be independently verifiable, and open-source routing logic may be inspected, tested, and replicated. A front-end that scans multiple automated market makers for available and already-committed liquidity, then helps the user build a draft transaction for a multi-path swap, may therefore be doing nothing more than transparently and deterministically reorganizing otherwise public information into a form the user can choose to act on. In that setting, the developer looks much more like the publisher of a tool than like a professional exercising judgment on the user's behalf. The harder cases arise where the operator relies on nonpublic information, makes claims about opaque or closed-source routing logic that users cannot readily verify, or otherwise asks users to place trust in ongoing discretionary decisionmaking that cannot be independently checked. It is

[130] Bloomberg Terminal is not the reason Bloomberg affiliates have to register with the SEC or CFTC. Rather, affiliates such as Bloomberg Tradebook LLC, Bloomberg SEF LLC, and Bloomberg STP LLC face registration obligations because they provide regulated market-intermediation, trading-venue, and post-trade infrastructure services. By contrast, Bloomberg Terminal primarily provides information, analytics, communications, and workflow tools that users leverage themselves.

there, and not merely wherever software makes financial action easier, that reasonable reliance on professional conduct begins to creep in.

The most difficult interface cases arise when the interface depends on operator-controlled service layers that can do more than inform. Default or mandatory RPC endpoints, proprietary routing APIs, relayers, backend orderflow management, transaction sequencing logic, and similar chokepoints may create the practical ability to steer, refuse, prioritize, or block user actions. Those capabilities matter. But even here, infrastructure alone cannot be the test. Every modern publisher operates infrastructure. Newspapers operate websites. Bloomberg operates servers and APIs. GitHub operates repositories. If server operation alone created professional conduct, software and data publication as such would become perpetually licensable.

The correct distinction is therefore not infrastructure versus no infrastructure. It is *communications infrastructure* versus *transactional authority*. An RPC provider that merely relays user-signed messages remains much closer to an internet service provider (ISP) or communications intermediary than to a broker, principal, or adviser. The user still chooses the transaction. The user still signs it. The provider cannot rewrite its terms. It is not acting as the user's agent merely because it relays the user's message.

The case changes when the operator can do more than relay information. A backend service that can steer routes based on hidden preferences, exclude venues, refuse execution, reorder transactions for economic effect, selectively privilege certain counterparties, or continuously optimize user positions begins to substitute the operator's judgment for the user's. At that point, the service layer starts to look less like publication and more like a managed intermediary function. The issue is not that the interface has become more "functional." The issue is that the operator may now be exercising a live role in the execution and management of user transactions rather than merely publishing tools for the user's own use.

Some of the most concrete modern examples of this line being muddled have appeared not in adjudicated cases, but in recent federal rulemakings. The SEC attempted to redefine "exchange" in ways that would have treated the mere "making available" of protocols, interfaces, and communication systems as exchange operation.[131] The IRS also attempted to impose broker-style reporting duties on software developers, communications intermediaries,

[131] *See, e.g., Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of "Exchange"*, 88 Fed. Reg. 29,448, 29,468–69 (proposed May 5, 2023) (to be codified at 17 C.F.R. pts. 232, 240, 242 & 249) (proposing to expand the definition of "exchange" to include systems that make available "communication protocols" and interfaces used to bring together buyers and sellers of securities).

and interface operators who lacked any ordinary customer-agent-or-principal relationship and who would therefore have needed to redesign their tools to become data-collection points.[132] Those episodes are worth examining in their own right, not because they announce controlling law, but because they show how easily regulators slip from regulating genuine intermediary conduct into regulating the publication and design of software itself. The next subsection takes up those two examples directly.

Across node clients, smart contracts, and user interfaces, the governing rule remains the same. The line is not usefulness, functionality, nor profitability. It is not the mere operation of servers or APIs. It is the point at which the developer or operator ceases to be a publisher of general tools and begins, in the law's older and more precise sense, to take the affairs of another in hand.

C. Two Recent Rulemakings That Crossed the Constitutional Line

The distinction between publication and professional conduct is not merely theoretical. In recent years two federal agencies proposed rules that illustrate, in unusually clear form, the temptation to regulate conduct by first regulating software publication. In one, the Securities and Exchange Commission proposed to redefine "exchange" in a way that threatened to convert the mere making available of communication protocols and trading interfaces into licensable exchange activity. In the other, the Treasury Department proposed to redefine "broker" in a way that threatened to impose reporting obligations on software developers, website operators, smart-contract publishers, and communications intermediaries who were not acting as customer agents or principals and who would therefore have had to redesign their tools in order to collect information they did not already possess.

Neither proposal ultimately became a durable precedent. The SEC's rule was later withdrawn. Treasury's broker rule was later repealed by Congress. But those later political outcomes do not diminish their analytic value here. Each proposal shows how easily regulators can slip from regulating actual intermediary conduct into regulating the publication and design of software itself. Each also provides a concrete example of where the constitutional line described in the previous sections is crossed.

i. The SEC's exchange-definition proposal

[132] *Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales*, 89 Fed. Reg. 106,928, 106,938–41 (Dec. 30, 2024) (to be codified at 26 C.F.R. pt. 1) (extending broker reporting obligations to certain digital asset service providers, including parties that facilitate transactions without traditional customer relationships).

The SEC's proposed amendments to the definition of "exchange" are the cleaner example of the two because the constitutional defect appeared at the threshold for who must register. The proposal altered the existing definition in two especially consequential ways. First, it shifted the focus from "bringing together orders" to "bringing together buyers and sellers." Second, it shifted the focus from "using" methods to "making available" various methods, including "communication protocols."[133]

Those changes mattered because they moved the rule away from conduct and toward publication. The existing exchange rule, whatever its constitutional limits, at least purported to regulate the conduct of using established methods to effectuate trades. Whereas the proposed rule instead attached registration obligations to the making available of "communication protocols," that is, to the publication of rule sets that allow others to communicate, negotiate, and agree to the terms of trade. The proposal itself repeatedly described those protocols as rules: rules governing message content, timing, recipient scope, instrument type, minimum order size, or the organization of displayed trading interest. In other words, what the proposal called "communication protocols" were, in essence, published instructions for interaction.[134]

That shift is constitutionally important for the reasons already discussed. To "use" methods to effectuate a trade is at least plausibly conduct. To "make available" communication protocols is mere publication. The proposal therefore risked transforming a conduct-based registration requirement into a speech-based one. Nor was the risk hypothetical. The proposal expressly stated that a communication-protocol system could qualify as an exchange even if it played no role in matching counterparties, displayed no trading interest, and hosted no execution. It was enough that buyers and sellers agreed to the terms of the trade "on the system," even if the publisher's role stopped at system publication.[135]

That is the constitutional line being crossed. A rule may, in some circumstances, require registration of entities that actually operate a market in the traditional sense. But a rule that requires a speaker to preregister before publishing protocols, rule sets, or interfaces because others may use those publications to communicate and transact is a prior restraint on speech. It is one thing to regulate a person who actually uses methods to match counterparties or stands in an intermediary role with respect to their transactions. It is another to say that one becomes an exchange merely by making available speech content, or instructions, that helps others coordinate.

---

[133] *Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems*, 87 Fed. Reg. 15,496, 15,504–08 (Mar. 18, 2022); Coin Ctr., Comments to the Sec. & Exch. Comm'n on Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems 2–6 (Apr. 14, 2022).
[134] 87 Fed. Reg. at 15,506–08; Coin Center, Exchange Comment at 4–7.
[135] 87 Fed. Reg. at 15,507 n.116; Coin Center, Exchange Comment at 5–6.

The proposal's own internal logic confirms the point. Its distinction between covered and uncovered activity did not turn on whether the publisher was engaging in some separate conduct in addition to publication. It turned instead on the content and design of the protocols themselves. Publishing rules that facilitate "general connectivity" might fall outside the definition, while publishing rules that facilitate communication among buyers and sellers about securities could fall inside it. The decisive factor was thus *what* the speaker chose to say in code. The proposal made the content of the rules, and the way those rules were "designed," the basis for registration. That is a content-based and speaker-based prior restraint on publication.[136]

The proposal also illustrates why the line between publication and professional conduct must be drawn functionally rather than rhetorically. To describe a protocol publisher as "bringing together buyers and sellers" sounds more like market operation than publication, but that verbal move cannot do the constitutional work. Buyers and sellers may indeed be brought together through speech. A newspaper advertisement may bring together a buyer and a seller. A bulletin board may do so. A website may do so. A public talk may do so. We should expect and perhaps even hope that politicians will *bring together* their audience rather than driving them further apart. But the fact that speech causes people to coordinate does not transform the speech into a regulated intermediary practice. If it did, the publication of classified ads, price sheets, and market commentary would always sit within the licensing power of the state.

The SEC proposal therefore crossed the constitutional line at the point where it ceased to regulate actual exchange operation and instead sought to regulate the publication of the rules and interfaces through which decentralized systems can be used. It did not ask whether the publisher had taken any user's affairs in hand. It did not ask whether the publisher was acting as agent, principal, adviser, or custodian. It did not ask whether the publisher was exercising judgment on behalf of a client. It asked instead whether the publisher had made available a communication protocol designed in a way that might allow others to trade. That is not the regulation of professional conduct. It is the regulation of speaking and publishing as such.

ii. Treasury's broker-reporting proposal

Treasury's broker proposal crossed the line in a different but equally revealing way. The exchange proposal threatened to require registration before publication. The broker proposal threatened to compel the redesign of software so that speakers who were not brokers in the traditional sense would become data-collection points for the government.

[136] 87 Fed. Reg. at 15,507–08; Coin Center, Exchange Comment at 5–7.

The existing broker rules hinge on whether a person "effects" sales for "customers," and the terms "effect" and "customer" have long been defined in agency-inflected ways. A person effects a sale by acting as an agent for a party in the sale or as a principal in the sale; a customer is the person for whom the broker acts as agent, with whom the broker acts as principal, or to whom the broker pays or credits the proceeds. The traditional structure is therefore tied to what might fairly be called the customer-agent-or-principal relationship.[137]

That existing standard fits both the statutory text and the Constitution. Where a person is in fact acting as a customer's agent, as a principal in a sale to the customer, or as a payor of proceeds, the government has a strong basis for imposing recordkeeping and reporting obligations. The speaker's conduct is independently regulable, she owes her client a duty and acts on her client's behalf. The information to be reported is ordinarily already in the speaker's possession by virtue of that conduct and relationship. And the resulting burden on speech is plausibly incidental to the regulation of genuine intermediation.

Treasury's proposal departed from that standard. It threatened to extend broker obligations to "digital asset middlemen," a newly defined category broad enough to sweep in persons who merely publish software, maintain websites, operate smart contracts, or otherwise provide access to tools used by others in peer-to-peer trading. It also proposed digital-asset-specific concepts that turned not on agency or principal relationships but on whether a speaker's software "provides access" to other tools or puts the speaker "in a position to know" information about users and transactions.[138]

That is where the constitutional defect emerged. Applying reporting duties to true intermediaries is one thing. Applying them to speakers who are not customer agents or principals, and who do not already possess the required information, is another. In that setting, the rule does not merely require a speaker to disclose facts already obtained in the ordinary course of a preexisting intermediary role. It compels the speaker to redesign the product so that the information will be collected in the first place. The proposal would have required software developers to rewrite wallets, websites, and smart-contract tooling so that users' names, identifying details, and transaction information could be gathered and reported even though the developers otherwise had "no reason or desire to collect" that information and no traditional customer relationship that made such collection incidental to their business.[139]

---

[137] 26 C.F.R. § 1.6045-1(a)(2), (10); Coin Center, Comments to the Department of Treasury on Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions 4–8 (Nov. 9, 2023).
[138] 88 Fed. Reg. 59,576, 59,586, 59,631–34 (Aug. 29, 2023); Coin Center, Broker Comment at 3–18.
[139] Coin Center, *Broker Comment* at 14–19.

That is not an incidental burden on professional conduct. It is a compelled redesign of expressive software. The law's leverage does not come from a separate, legally operative role the speaker has already assumed. It comes from forcing the speaker to alter the architecture and capabilities of the publication so that a new role comes into being. Put differently, the state would not be regulating a broker who already stands between the user and the market. It would be ordering a publisher to *become* such a person.

That distinction is particularly important in crypto because many tools are deliberately designed so that users can act for themselves without any agency relationship or legal trust-based relationship with the publisher. That is often the whole point of the architecture. The user signs their own messages. The protocol validates them. The software helps the user act for themself. Treasury's proposal effectively sought to reverse that architecture by compelling developers to redesign their tools such that an agency-like relationship would have to be introduced between the author of the tool and its users. The constitutional line is crossed precisely there. The burden is no longer incidental to conduct; it is aimed at changing speech products into intermediated services.[140]

The proposal also shows why the mere existence of a business model is not enough. Treasury argued that software publishers earning fees from usage are engaged in business and can therefore be required to gather more information. But every serious publisher is engaged in business. Newspapers charge subscription fees. Bloomberg charges terminal fees. Software companies charge license fees. Those facts do not convert publication into brokerage. Even where a developer is compensated automatically through software, that alone does not create a customer relationship in any traditional sense where the user and publisher have formed a contractual or agency relationship.[141] Taken seriously, Treasury's theory would collapse the distinction between publishing and intermediation altogether, allowing the state to demand that ordinary publishers build systems to identify and track their audiences.

Nor did the proposal avoid the First Amendment problem by framing the compelled reports as private disclosures of non-controversial facts to the IRS and the taxpayer. The real burden did not lie only in the ultimate reporting form. It lay earlier, in the requirement that publishers of software tools and websites build entirely new systems for gathering information that they did not already possess. That is why the issue cannot be reduced to the constitutional doctrines of ordinary factual disclosure. The state was not merely demanding existing facts; it was compelling the creation of software embodying a different vision of privacy, identity, and financial architecture.

---

[140] Coin Center, *Broker Comment* at 18–19.
[141] Coin Center, *Broker Comment* at 14 n.40.

iii. The common defect in both proposals

The SEC and Treasury proposals differed in mechanism, but not in constitutional logic. The SEC proposal moved the exchange definition from conduct toward publication by shifting from "using" methods to "making available" protocols. Treasury moved broker reporting from actual intermediaries toward speakers by extending obligations to those who would have to redesign their tools in order to become information intermediaries. In each case, the agency sought to regulate actual financial conduct by first controlling what kinds of software, interfaces, and protocols may be published and how they must be designed.

That is the common defect. The state may regulate actual brokers, exchanges, advisers, custodians, banks, and other intermediaries where those roles genuinely exist. The state may dislike the fact that self-help tools and decentralized systems allow people to transact without traditional intermediaries, but it may not solve that perceived problem by pretending that the publisher of the tools is the absent intermediary. That would be speech regulation and the Constitution does not permit that substitution.

These two proposals are therefore useful not because they announce controlling law, but because they make visible the pressure points in this area. When agencies stop asking whether a person has taken another's affairs in hand and begin asking instead whether a person has published useful protocols or interfaces that others may use to trade, the First Amendment problem has already appeared. When agencies stop requiring reports only from actors who already possess customer information by virtue of a genuine intermediary role and additionally require software publishers to redesign their tools so that they will begin collecting that information, the line has already been crossed.

That, in the end, is the lesson of the prior sections. The law should regulate real intermediaries where real intermediation exists. It should not turn publication, software maintenance, communication protocols, or user-facing design into professional conduct by regulatory fiat. To do so is to license and compel speech based on content such that the only speech remaining expresses a government-preferred viewpoint. It is nakedly unconstitutional.

VI. Conclusion

The First Amendment application to crypto software publication is not as novel as it may initially appear. The Supreme Court has already answered the core questions. The creation and dissemination of information is protected speech. Content-based restrictions, compelled speech, and prior restraints are sharply limited. And regulation of professional conduct is permitted only where a speaker has moved beyond publication and assumed a role of agency, custody, or delegated judgment over the affairs of another.

This paper has shown that crypto software publication fits squarely within that framework. Whether that software is a blockchain node client, a smart contract, or a purely informational or user-controlled UI, the act of writing it and making it publicly available is itself the creation and dissemination of information. And whether that information is technical, executable, or commercially relevant does not weaken these First Amendment protections. The Supreme Court has never treated usefulness or functionality as a basis for diminished protection. If anything, its cases point the other way.

The contrary view rests on a category error. It treats publishers as operators and fiduciaries simply because others use their publications to act. But that is not how we treat speech in any other domain. We do not convert cookbook authors into chefs, mapmakers into sailors, or investment newsletter publishers into licensed advisers simply because their speech is useful and effective. The same principle applies here. The government may impose on those who actually take the affairs of others in hand. It may not collapse that category of conduct into the mere act of publishing software.

Crypto software allows individuals to act for themselves in ways that once required intermediaries. That shift may pose challenges for regulatory frameworks built around those intermediaries. It may reduce visibility, control, or leverage. But constitutional protections do not yield to administrative convenience. The state may regulate real intermediaries where they exist. It may not respond to their absence by declaring the speakers who built self-help tools to be the missing middlemen.

This final point matters for more than just crypto software. If the government is allowed to dictate how software is written, then the freedom to convey technical knowledge, organize social and economic life, and embody deep political judgments on matters of privacy and autonomy becomes contingent on the goodwill of the government. This would not only constrain scientific progress in the United States, but also suffocate political and economic freedom. The First Amendment does not permit that.

Instead, where a person speaks into the world by publishing software that others can use, this person is engaged in protected speech. Where a person undertakes to serve as an agent, custodian, or take the affairs of a client personally in hand and purport to exercise judgment on behalf of the client, regulation may be attached to such conduct. Keeping those categories distinct is the only way to maintain the integrity of the First Amendment and the government's legitimate authority and responsibility to protect consumers and investors.

Crypto software does not necessitate the invention of new legal doctrines or novel carveouts. It requires the faithful application of settled First Amendment principles to a new technological context. In the age of computers, where software is the primary means for expressing ideas and organizing economic life, those principles matter more, not less. Writing and publishing code is speech. And in a free society, speech cannot be licensed into silence.