Electronic Cash, Decentralized Exchange, and the Constitution

Peter Van Valkenburgh
March 2019

Coin Center Report

COIN CENTER
coincenter.org

Peter Van Valkenburgh, *Electronic Cash, Decentralized Exchange, and the Constitution*, Coin Center Report, Mar. 2019, available at https://coincenter.org/entry/e-cash-dex-constitution

Abstract

Regulators, law enforcement, and the general public have come to expect that cryptocurrency transactions will leave a public record on a blockchain, and that most cryptocurrency exchanges will take place using centralized businesses that are regulated and surveilled through the Bank Secrecy Act. The emergence of electronic cash and decentralized exchange software challenges these expectations. Transactions need not leave any public record and exchanges can be accomplished peer to peer without using a regulated third party in between. Faced with diminished visibility into cryptocurrency transactions, policymakers may propose new approaches to financial surveillance. Regulating cryptocurrency software developers and individual users of that software under the Bank Secrecy Act would be unconstitutional under the Fourth Amendment because it would be a warrantless search and seizure of information private to cryptocurrency users. Furthermore, any law or regulation attempting to ban, require licensing for, or compel the altered publication (*e.g.* backdoors) of cryptocurrency software would be unconstitutional under First Amendment protections for speech.

Author

Peter Van Valkenburgh
Coin Center
peter@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. 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. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Acknowledgements

Thank you to Andrea Castillo who provided invaluable research assistance, and to my Coin Center colleagues Neeraj Agrawal, James Foust, Robin Weisman, Alex Strernhell, and Jerry Brito for indispensable discussions and comments on early drafts of this paper. Sincere thanks to those who provided comments on a draft of this paper, including Brandon G. Goodell, Jason Somensatto (0x Project), Alexander Zaidelson (Beam), Elena Nadolinski (Beanstalk), Ron Bernstein (Coinbase), Rainey Reitman & Jamie Lee Williams (Electronic Frontier Foundation), Silke Elrifai (Gnosis), Daniel Lehnberg (Grin), Alex Gladstein (Human Rights Foundation), Steven Waterhouse (Orchid Labs), Marvin Ammori (Protocol Labs), Alan Curtis (Radar), Zooko Wilcox (Zcash), and Josh Cincinnati (Zcash Foundation). Special thanks to Shane Glynn, Joshua Goldbard, and Nathana Sharma (MobileCoin) for helping organize a workshop for this paper.

Table of Contents

I. Introduction and Executive Summary **4**

II. Technology Background **9**

A. Electronic Cash Means Completely Private, Cash-Like Transactions 10

B. Decentralized Exchange Means No Trusted Third Party 12

C. Electronic Cash and Decentralized Exchange are Powered by Software 15

III. Electronic Cash, Decentralized Exchange, and the Fourth Amendment **17**

A. Fourth Amendment Protections Apply to Electronic Messages 17

B. The Third-Party Doctrine 20

C. The Bank Secrecy Act 24

D. The Constitutionality of the Bank Secrecy Act 26

E. Regulating Software Developers Under the BSA Would be Unconstitutional 30

IV. Electronic Cash, Decentralized Exchange, and the First Amendment **32**

A. Computer Code is Protected Speech 33

i. Computer Code Expresses Ideas for Political and Social Change 33

ii. Publishing Computer Code is a Speech Act, Not Symbolic Conduct 35

iii. Electronic Cash and Decentralized Exchange Software Are Protected Speech 37

B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech 39

C. Regulating Publication of Electronic Cash and Decentralized Exchange Software 45

i. Banning Publication Would be Unconstitutional 46

ii. Licensing Regimes for Publication Would be Unconstitutional 49

iii. Compelling Developers to Write Backdoors Would be Unconstitutional 51

V. Conclusion **53**

Appendix: Building Electronic Cash and Decentralized Exchange Software **55**

Integrity and Privacy: The Quarrelsome Core Design Goals of Cryptocurrencies 55

Early Attempts at Electronic Cash 58

Brief Overview of Electronic Cash Efforts Thus Far 61

Characterizing the Development Process 64

An Example of What Gets Built: Digital Signature Schemes 64

Who Builds this Software? 69

If a developer of electronic cash or decentralized exchange software publicly announced that they were voluntarily incorporating BSA-style surveillance into their tools, users who continued to use those tools would likely lose their reasonable expectation of privacy over any information they provided when they used those tools. However, it is hard to imagine that *every* developer of electronic cash or decentralized exchange software would suddenly choose to voluntarily surveil the users of their software, even under pressure from law enforcement (many are not located in the U.S.). It is even more unbelievable that users would continue to use tools that had known backdoors if previous versions of the software without backdoors continued to exist in online archives or on peer-to-peer file sharing networks, or if other developers continued to offer more private alternatives.

If a developer refused to comply with a regulator's demand that they add surveillance backdoors into their tools and the regulator either ordered them to cease publishing their software or compelled them to add the backdoor through a legal order then two additional constitutional questions would surface:

1. Is a licensing requirement or ban on the publication of electronic cash or decentralized exchange source code an unconstitutional prior restraint on protected speech?
2. Is an order to only publish electronic cash or decentralized exchange source code with surveillance backdoors unconstitutionally compelled speech?

To answer these questions and the perfunctory matter of whether electronic cash or decentralized exchange source code is constitutionally protected speech, we must turn from the Fourth Amendment to the First.

IV. Electronic Cash, Decentralized Exchange, and the First Amendment

The First Amendment prohibits the content-based regulation of expressive speech unless the government can prove a compelling state interest that could not be achieved through any less restrictive policy.[147] If electronic cash or decentralized exchange source code is expressive speech, then a publication ban or licensing requirement on developers would be presumed unconstitutional unless the government can prove in court that banning that software or licensing its publication achieves a compelling state interest that could not be achieved through any less restrictive policy. Similarly there would be a presumption of unconstitutionality if a law or regulation attempted to compel developers to rewrite their source code to include backdoors.[148]

Rarely do courts faced with bans on speech of a certain type or content find that the government's interest is truly compelling and not achievable through less restrictive policies. Therefore, cases usually hinge on whether the speech is indeed protected and what level of protection it deserves. The remainder of this report argues that electronic cash and

[147] This judicial review standard is known as "strict scrutiny" and is used to evaluate constitutionality. *For more, see*: Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. Rev. 1267 (2006-2007).
[148] *See infra* IV. C. iii. Compelling Developers to Write Backdoors Would be Unconstitutional, pp. 51-52.

decentralized exchange source code is protected speech and that laws banning or requiring licensing for its publication, as well as laws compelling developers to alter their speech, should be presumed unconstitutional and must face strict scrutiny, rather than a lower standard such as intermediate scrutiny, upon judicial review.

A. Computer Code is Protected Speech

The Supreme Court has yet to hold generally that programs written in computer code are protected speech. However, holdings in cases dealing with novels, musical scores, and blueprints strongly suggest that computer code would be protected speech, and two recent cases related to video games and prescription datasets establish broad tests for whether any electronic data (software included) would qualify as protected speech. Lower courts have taken varied approaches, and some have found that computer code is protected speech because it is expressive conduct, like flag burning or nude dancing. As we shall discuss, this conduct-based approach has split the circuits, is misguided, offers lesser protection from regulation, and has no support in Supreme Court precedent.

i. Computer Code Expresses Ideas for Political and Social Change

In *Roth v. United States*, the Supreme Court found that "the First Amendment was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[149] Generally, the particular medium through which ideas are expressed is inconsequential to First Amendment protection. If it is an idea of at least modest "political and social" significance, the Court certainly does not discriminate.[150] It protects ideas regardless of the medium in which they are presented, even if it is gibberish or visual chaos. As the Court has found, the category of "unquestionably shielded" speech includes a "painting of Jackson Pollock, music of Arnold Schöenberg, or Jabberwocky verse of Lewis Carroll."[151]

As discussed earlier,[152] open source computer code shared over the internet is directly intended to convey the scientific and engineering ideas of a given project to other developers, including current collaborators, potential future collaborators, researchers, and the general public who may wish to use these tools and seek assurances of their correct operation, which can only be achieved through publicity and transparency. If digital tools derived from this science and engineering will be employed to, for example, organize social behavior on the internet, then their source code certainly holds at least as much social and political significance in the 21st century as a schematic of a steam engine or a blueprint for an amphitheater would have held in previous ages.

---

[149] *Roth v. United States*, 354 U.S. 476 (1957) https://supreme.justia.com/cases/federal/us/354/476/.
[150] *Ibid.*
[151] *Hurley v. Irish-American Gay, Lesbian & Bisexual Group of Boston,* 515 U.S. 557, 569 (1995) https://supreme.justia.com/cases/federal/us/515/557/.
[152] *See supra* II. C. Electronic Cash and Decentralized Exchange are Powered by Software, pp. 15-17.

Indeed, the "unfettered interchange of ideas"[153] found in computer code is the primary motivation behind open source software development as a practice. Rather than cloister one's software project within the developer staff of a single corporation by enforcing copyrights, trade secrets, and other restrictions on dissemination through a proprietary software model, open source software development principles eschew copyrights and restrictive licenses, push for better ways to clearly and publicly display source code for review, and seek to solicit the widest possible audience in order to increase the odds that a member of that audience will catch errors that would otherwise go undetected or find opportunities for innovation that would otherwise have been ignored. This ethos is long established and well-captured in developer Eric Raymond's landmark 1997 essay *The Cathedral and the Bazaar*.[154] All major electronic cash and decentralized exchange software projects rigorously adhere to this open source model of development. Canonical changes to that software are only made after an exhaustive round of public sharing and discussion of the code itself.[155]

Moreover, computer code underlies systems we rely upon daily to organize our society—from email clients to traffic lights, police surveillance cameras to social networking websites and—more recently—private decentralized money and exchange. Everything we do (and cannot do) on those platforms and with those tools is mediated by software and ideas expressed in

---

[153] *Roth v. United States*, 484.

[154] In the essay, Raymond explains several emergent rules in the open source developer community: "Every good work of software starts by scratching a developer's personal itch." The majority of developers in an open source project are motivated primarily because they want to use the product they are making. They aren't under contract to build something for someone else; they have a personal need and they are addressing it. This leads to greater motivation and it brings intimate personal knowledge about the problem to bear. "Good programmers know what to write. Great ones know what to rewrite (and reuse)." When development happens in the open, redundancy can be avoided, a division and specialization of knowledge and expertise achieved, and troublesome, complicated, or redundant code identified and simplified. "When you lose interest in a program, your last duty to it is to hand it off to a competent successor." People come and go within an open source project depending on their interests and expertise. No one gets stuck working on projects they no longer care about and fresh minds appear to offer different perspectives on longstanding problems or new avenues for development. "Treating your users as co-developers is your least-hassle route to rapid code improvement and effective debugging." Many of the people who use the open source code will also be able to identify and flag issues, and may even be able to offer solutions. The line between a consumer and a producer of open source software blurs because production happens transparently in full view of the public and participation in production is available to all. "Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone." This has come to be known as Linus's Law after Linus Torvalds, the original creator and longtime principal developer of Linux. When development is not open, all developers may share a certain blind spot or fail to notice a certain error. Wider development amongst sophisticated users with idiosyncratic perspectives increases the likelihood that bugs are discovered and addressed, thus making open source software more resilient and secure. *See*: Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Cambridge, MA: O'Reilly, 1999.

[155] *See, e.g.*: the so-called block size debate among the Bitcoin community. *For an overview, see*: Aaron van Wirdum, "Segregated Witness, Part 3: How a Soft Fork Might Establish a Block-Size Truce (or Not)," *Bitcoin Magazine* (Dec 29, 2015) https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-soft-fork-might-establish-a-block-size-truce-or-not-1451423607/.

code. Anyone can learn to read the languages in which this code is written in order to elevate and formulate their view of debates surrounding these technologies, and anyone who has learned those languages can invent and suggest new and different ideas, including alternatives to the systems of today. Developers may learn these skills because they think they can build better, safer tools for organizing society, enabling individual freedom, or limiting the freedom of those who would do others harm.

Say what one will about the deservedly mocked mantra of Silicon Valley, "make the world a better place," but software does make the world.[156] Source code and the creative and scientific expression it contains now represents a substantial quantity of the world's "ideas for the bringing about of political and social changes desired by the people."[157] Many remain surprised and even alarmed that a new language—many new languages in fact—are actively being used to fundamentally reshape the landscape of human interaction. But to deny this fact is to deny everything that has changed in our lives since the advent of digital computing. Similarly, to deny statements made in coding languages like C++[158] or Rust[159] the same protections we would grant statements made in English would make no more sense than to deny novels protection when they are written in French, symphonies protection because they are written in musical notation, or scientific papers protection because they tend to be filled with arcane graphs and formulae.

At least under the broad standard articulated by the Court in *Roth*, electronic cash and decentralized exchange software should be protected speech. A rigorous analysis, however, is not that simple. As we shall unpack in the next two subsections, some lower courts have muddled what should be a straightforward analysis by treating code as expressive conduct rather than speech, meaning it is subject to weaker First Amendment protections. By contrast, recent Supreme Court cases have eschewed this conduct-based approach and articulated extremely broad tests for what qualifies as strongly protected speech in the digital age. Later we will describe the different levels of protection (*i.e.* strict vs. intermediate scrutiny) to which various types of expression (*i.e.* expressive conduct vs. speech) are entitled, and the importance of this seemingly academic debate will be clear: if electronic cash or decentralized exchange software is found to be expressive conduct rather than speech it is entitled to substantially weaker protections.

ii. Publishing Computer Code is a Speech Act, Not Symbolic Conduct

The Supreme Court has yet to hold generally that programs written in computer code are protected speech. That said, it has also never explicitly found that short stories written in Russian are protected speech or that oboe concerti written in musical notation are protected

---

[156] *See, e.g.*: "Silicon Valley, TechCrunch Disrupt Parody," *goodlaugh182 YouTube Channel* (May 25, 2014) https://www.youtube.com/watch?v=J-GVd_HLlps.
[157] *Roth v. United States, 484.*
[158] *See, generally:* Bjarne Stroustrup, "The Essence of C++," *The University of Edinburgh YouTube Channe*l (May 4, 2014) https://www.youtube.com/watch?v=86xWVb4XIyE.
[159] *See, generall*y: Steve Klabnik and Carol Nichols, *The Rust Programming Language*, San Francisco, CA: No Starch Press (2018) *available at* https://doc.rust-lang.org/book/ch00-00-introduction.html.

speech. Some lower courts have begun to analyze this question under the jurisprudence of expressive conduct.[160] These cases rely on the *Spence*[161] and *O'Brien*[162] tests for expressive conduct developed in earlier holdings from the Court. As we will argue later at length, these lower-court applications of *Spence* and *O'Brien* are misguided approaches to the question of whether computer code is protected speech. Those cases dealt with actions, not mere ideas: hanging a flag upside down in *Spence*,[163] and burning a draft card in *O'Brien*.[164] Actions may be expressive, but they can also have more immediate and dangerous consequences than mere words. Burning a building down may express someone's feelings about that building, but it also presents obvious risks to life and property. Therefore, even if a expressive action, like burning a flag, is found to be speech, it will often be entitled to less-strict protection from regulation.

Computer code, however, is not an expressive or symbolic action. It is, quite literally, a written series of symbols themselves, *i.e.* letters and numbers or, once compiled, 0s and 1s. It is not like a musical performance, but rather like the printed score for an orchestra's conductor or the printed roll for a player piano. While it is true that people will use computer source code to perform actions (just as one might use the musical score to perform music), the act of writing and sharing the code is an entirely separate act from the act of executing the code. Each or both may be protected speech, but they must be analyzed separately: analysis of the act of executing the code must use the *Spence* and *O'Brien* tests for expressive conduct, and analysis of the act of writing and sharing the code must use the same standards we use for authorship of novels or musical scores as articulated in *Roth*.[165] To conflate the analysis and judge both the authorship and execution of code under *Spence* and *O'Brien* is to treat an impromptu performance of the 1812 Overture (cannons and all) the same as the moment Tchaikovsky put pen to paper on his musical score. The potentially disruptive performance should rightly and constitutionally be subject to somewhat prescriptive regulation, while the mere act of writing the music in notes and clefts on paper should not.

As we have discussed, making electronic cash or decentralized exchange transactions involves executing computer code. We do not argue in this report that the act of executing that code and actually transmitting or exchanging cryptocurrency is protected speech. (It may be protected speech in several contexts, but if we were making this argument we would likely need to use the *Spence* and *O'Brien* tests to determine whether a symbolic action is protected speech.) This report is concerned only with the developers of computer code and whether they can be banned from publishing code, made to get a license to publish it, or compelled to alter the code they publish such that it has surveillance backdoors. Although it is unlikely, a developer of electronic cash or decentralized exchange software may go her whole life without making an electronic cash transaction or a decentralized exchange. The question of whether she deserves

---

[160] *Universal City Studios, Inc. v. Corley* , *Junger v. Daley*, and *Karn v. US Dept. of State*.
[161] *Spence v. Washington,* 418 U.S. 405 (1974) https://supreme.justia.com/cases/federal/us/418/405/.
[162] *United States v. O'Brien,* 391 U.S. 367 (1968) https://supreme.justia.com/cases/federal/us/391/367/.
[163] *Spence v. Washington*.
[164] *United States v. O'Brien*.
[165] *Roth v. United States*.

First Amendment protection hinges not on what actions others may use her software to perform but merely on whether she, simply by publishing, has engaged in protected speech.

iii. Electronic Cash and Decentralized Exchange Software Are Protected Speech

In two cases, *Brown v. Entertainment Merchants Association*[166] and *Sorrell v. IMS Health Inc.*,[167] the Supreme Court has found that some computer programs and some digital data are worthy of protection as speech. It did not use the *Spence* or *O'Brien* test in either determination.

In *Brown*, the court found that video games were protected speech and even violent ones could not be banned from sale. Some scholars believe that *Brown* articulated a new, narrow standard for when novel modes of expression would be entitled to First Amendment protections.[168] For example, lawyer Andrew Tutt writes:

> Rather than reach beyond video games to software generally, the Court zeroed in on video games and held that they were speech because they communicated ideas through familiar literary devices. The Court reasoned that video games were speech because they expressed ideas in familiar ways: "Like the protected books, plays, and movies that preceded them, video games communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)."[169]

Tutt views the Court's failure to analyze the underlying code itself, and its focus on the analogous content between video games and more traditional entertainments, as indicative of a narrow standard: "*Brown's* test is probably best read as defining 'new speech' as that which is directly analogous in presentation and mode to 'old speech.'"[170] Tutt, however, makes too much of this holding. The Court does not at any point hold that it is identifying a new standard that conflicts with or narrows previous interpretations, such as those in *Roth*. Instead, the Court holds that it is *sufficient* for a finding of protected speech that new modes of expression are analogous to old modes. At no point does the Court suggest that it is *necessary* for the new mode to bear this resemblance. As the Court held, resemblance "*suffices* to confer First Amendment protection."[171] Even if resemblance was now necessary rather than sufficient, open

---

[166] *Brown, et al. v. Entertainment Merchants Assn. et al.*, 564 U.S. 786 (2011) https://supreme.justia.com/cases/federal/us/564/786/.
[167] *Sorrell, et al. v. IMS Health Inc., et al.*, 564 U.S. 552 (2011) https://supreme.justia.com/cases/federal/us/564/552/.
[168] *See*, *e.g.*, Andrew Tutt, *Software Speech*, 65 Stan. L. Rev. Online 72 (2012) https://www.stanfordlawreview.org/online/software-speech/.
[169] *Ibid.*
[170] *Ibid.*
[171] Emphasis added. *Brown, et al. v. Entertainment Merchants Assn. et al.*, 788.

source software would easily be analogous to scientific publications shared amongst experts, which are protected as speech.[172]

In *Sorrell*, the Court articulated a surprisingly broad standard of what constitutes protected speech. It found that the mere "creation and dissemination of information" constitutes speech within the meaning of the First Amendment.[173] *Sorrell* dealt with a law that "on its face" enacted "content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information."[174] The Court found that a Vermont law limiting sales of and access to records of which medicines doctors prescribe "disfavors marketing, that is, speech with a particular content" and "disfavors specific speakers, namely pharmaceutical manufacturers."[175] Vermont contended that the sale, transfer, and use of prescriptions data was conduct and not speech (as we discussed earlier and will return to in the next section), but the Court rejected this argument out of hand, adding that:

> 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.[176]

The computer code within electronic cash and decentralized exchange systems is heavily laden with facts that advance human knowledge and allow us to conduct human affairs. If the essential factual nature of discrete logarithms was not well understood, to give one example, we would struggle to engage in any secure electronic conversations.[177] Bank records, government secrets, and copyrighted content would all be up for grabs if not for pioneering advances in the science of applied cryptography. These are advances that, by and large, have always been best uncovered and expressed in computer code.

Therefore, even though there is no conclusive holding from the Supreme Court on the specific topic of computer code's classification as protected speech, we can reasonably assume, based on older cases such as *Roth*[178] as well as recent holdings such as *Sorrell,* that the issue would be

---

[172] *See, e.g., FCC v. Pacifica Foundation*, 438 U.S. 726, 746 (1978) (words which lack literary, political, or scientific value are not entirely outside first amendment protection); *Miller v. California*, 413 U.S. 15, 34 (1973) ("The First Amendment protects works which, taken as a whole, have ... scientific value, regardless of whether the government or a majority of the people approve of the ideas these works represent."); *Roth v. United States*, 354 U.S. 476, 484 (1957) (quoting a letter of the Continental Congress identifying scientific progress as a reason for protecting speech).
[173] *Sorrell, et al. v. IMS Health Inc., et al*.
[174] *Ibid*.
[175] *Ibid*.
[176] *Ibid*.
[177] Kevin S. McCurley, "The Discrete Logarithm Problem," *Proceedings of Symposia in Applied Mathematics*, Vol. 42 (1990): pgs. 49-74, http://www.mccurley.org/papers/dlog.pdf.
[178] As the Court held in *Roth*, "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." *Roth v. United States*, 354 U.S. 476, 484, 77 S.Ct. 1304, 1 L.Ed.2d 1498 (1957).

non-contentious: it's protected. Setting aside the issue of expressive conduct vs. speech, every court of appeals to rule on this issue has held that code is protected expression worthy of at least some First Amendment protections.[179]

However, as we shall see in the next two sections, the finding that code is protected expression does not mean that it cannot be regulated. Much depends on the nature of the speech and the concomitant level of scrutiny that regulations impacting that speech will face.

B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech

As we have discussed, electronic cash and decentralized exchange software is protected under the First Amendment. However, not all protected expression is protected equally. For our purposes, there are two standards of review that courts may use to judge the constitutionality of laws regulating electronic cash or decentralized exchange software: strict scrutiny and intermediate scrutiny.

Strict scrutiny is formulated such that a law or regulation will be found unconstitutional unless it is "narrowly tailored to serve a compelling state interest."[180]

---

[179] For example, in *Universal City Studios v. Corley*, the Second Circuit held that "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment." Similarly in *Junger v. Daley*, the Sixth Circuit explained that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment." *See*: *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

[180] *See*, *e.g.*, *Austin v. Michigan Chamber of Commerce*, 494 U.S. 652, 655 (1990). Constitutional scholar Eugene Volokh has expertly captured the sweep of strict scrutiny jurisprudence. Eugene Volokh, Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny, 144 U. Pennsylvania L. Rev. 2417 (1997). We will include the salient parts here:

As Volokh writes, "The Court has set forth four general principles related to compelling interests."

1. Compelling interests cannot privilege certain broad social or political interests over others. As Volokh has observed, "The mere interest in furthering a subset of [economic, social, and political] speech (for instance, labor picketing) "without more, cannot justify [a content-based] exemption" for such speech.
2. The fact that restricting speech would avoid offence or squelch unpopular and disagreeable ideas cannot be a compelling interest. Volokh offers flag burning as an example, citing *Texas v. Johnson*.
3. An interest may reveal itself as non-compelling if the government refused to pass laws that would more effectively address the issue. Volokh offers the example of an Illinois law that attempted to ban labor protests. When the state attempted to justify the law by virtue of ensuring residential privacy, the Court found the lack of similar laws addressing disruptive protests for other political causes evidence that the residential privacy interest was not compelling.
4. An interest may reveal itself as non-compelling if the government's attempt to address it is woefully underinclusive. Volokh cites a case wherein a law prohibiting criminals from publishing memoirs was justified as preventing criminals from profiting from their crimes. The Court found that there were so many other ways to prevent such profiting left unaddressed, that the government evinced a lack of seriousness with respect to its purported compelling interest.

Intermediate scrutiny, on the other hand, is an easier hurdle for laws and regulations to clear. As the Second Circuit found in *Universal City Studios, Inc. v. Corley*, under intermediate scrutiny:

> The regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest.[181]

While this test may not appear drastically different from the strict scrutiny formulation above, in practice its application is significantly less charitable to speech. As constitutional scholar Ashutosh Bhagwat writes,

> [I]n applying intermediate scrutiny to reconcile governmental interests with free speech claims, the appellate courts have tended to systematically favor the government. Although the balance that the courts have drawn in individual cases is often perfectly defensible, and indeed may be an inevitable consequence of the form of analysis mandated by the intermediate scrutiny test, [we] show that the aggregate consequence of this governmental preference is the suppression of substantial amounts of important, socially valuable speech.[182]

Symbolic conduct, like burning a flag, is only entitled to intermediate scrutiny because of the obvious public safety issues inherent in actions rather than words. When the standard of review is intermediate scrutiny, laws regulating speech tend to be upheld as constitutional and speech can be suppressed.[183] Advocates for continued research and development of electronic cash and decentralized exchange software should not, therefore, accept that these tools are protected because they are symbolic conduct. Instead, they must argue that these tools are not conduct, but speech, and that their publication by developers is an entirely separate matter from their use by other persons to perform actions in the world. Aside from being more likely to garner strong constitutional protection, this approach is also correct.

With one exception, lower court judges have found that computer code is a hybrid of speech and conduct because it is "functional."[184] This a misguided approach that has not been adopted

---

Volokh, however, finds that the majority of strict scrutiny cases turn on the question of narrow tailoring, and recounts Court-articulated factors pertaining to that analysis:

1. A narrowly tailored law should, in fact, advance the compelling interest, but scientific proof is not required.
2. A narrowly tailored law must not restrict a significant amount of speech unrelated to the government interest.
3. If there is a less restrictive means to achieve the interest, then the law is not narrowly tailored.

[181] *Universal City Studios, Inc. v. Corley,* 273 F.3d 429 (2d Cir. 2001).

[182] Ashutosh Bhagwat, *The Test That Ate Everything*: *Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. Ill. L. Rev. 783 (2007).

[183] *Id*.

[184] The exception is *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt, *Cf. Universal City Studios, Inc. v. Corley*, *Junger v. Daley*, and *Karn v. US Dept. of State*, 925 F. Supp. 1 (D.D.C. 1996) https://law.justia.com/cases/federal/district-courts/FSupp/925/1/2294325/.

by the Supreme Court[185] and that should be avoided by electronic cash and decentralized exchange advocates.

For example, in *Junger v. Daley* the Sixth Circuit held that "[t]he fact that a medium of expression has a functional capacity should not preclude constitutional protection. Rather, the appropriate consideration of the medium's functional capacity is in the analysis of permitted government regulation."[186] At root, *Junger* suggests that if the code is functional then it is both conduct and expression. As expressive conduct, laws regulating its publication and distribution would be subject only to intermediate scrutiny thereby permitting more restrictive government regulation.

Some commentators[187] suggest that these lower court judges have misunderstood how software works by failing to understand the difference between source code, which is primarily used by developers to *express* new systems and share their ideas with other developers, and object code, the compiled form of source code that will actually trigger a computer to do something *functional*.[188]

Even if that was the case, and even if we accept that judges should be better at discriminating between the two types of code, why should object code be expressive conduct rather than speech? After all, object code is merely a unique and often important arrangement of digits or bits.[189] Returning to the musical metaphor, source code would be the composer's score, a piano roll would be the object code, and the player piano would be the computer. Object code can in fact be read by particularly sophisticated developers in order to understand a message.[190] Piano rolls too are used by musicians to share music; some may even be more adept at reading this

---

[185] *See Sorrell, et al. v. IMS Health Inc., et al.*

[186] *Junger v. Daley*.

[187] *See*: L Jean Camp, "Code as Speech: a discussion of Bernstein v. USDOJ, Karn v. USDOS, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism" *Ethics and Information Technology*, March 2001. Vol. 1, No. 2 *available at* http://www.ljean.com/files/CODE_FEDERALISM.pdf ("Judge Gwin's assertion that 'source and object code are essentially interchangeable' is simply wrong. His very next statement that 'source code is not directly executable by a computer' exposes his error. The error in Judge Gwin's understanding of how software works is further exposed in the footnote of the previously quoted passage: 'Software in source code, a 'high level language,' is unintelligible to most, but it can be understood by computer scientists, mathematicians, programmers, and others with knowledge of the particular language in which the program is written.")(*citing Junger v. Daley*).
See also: Adrianna Oddo, *Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection Against Compelled Speech* 67 Cath. U. L. Rev. 211 (2018) ("With respect to questions regarding computer code, courts must further distinguish whether the speech in question is source code or object code.").

[188] *Ibid.* L Jean Camp.

[189] It might look like this: 01101111 01110000 01100101 01101110 00100000 01110100 01101000 01100101 00100000 01110000 01101111 01100100 00100000 01100010 01100001 01111001 00100000 01100100 01101111 01101111 01110010 01110011.

[190] David S. Touretzky, "Source vs. Object Code, A False Dichotomy," *Carnegie Mellon University* (Jul. 12, 2000) https://www.cs.cmu.edu/~dst/DeCSS/object-code.txt.

style of musical notation than a traditional score.[191] Regardless of whether we're discussing dots and dashes on a roll of paper or 1s and 0s in a computer file,[192] how can the creation and dissemination of these unique arrangements of data be anything but the "creation and dissemination of information,"[193] which is the Supreme Court's standard for speech in *Sorrell*? The Oxford English Dictionary defines "information" as "what is conveyed or represented by a particular arrangement or sequence of things."[194]

Again, counter to the lower court in *Junger*, the Court in *Sorrell* felt no need to address Vermont's argument that prescription data was conduct, and held that "if 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."[195]

In *Corley*, at least, the district court judge (who was praised and quoted heavily by the Second Circuit)[196] did not appear to misunderstand software but rather felt that the ease with which an otherwise purely expressive piece of source code could be compiled into object code and executed by the user of a computer meant that, for all intents and purposes, the code should be regulated as conduct as well as expression.

As the district judge wrote:

> Computer code, ... no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really 'a proxy for effects or harm' and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.
>
> The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.
>
> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the

---

[191] *See, e.g.*: "Boogie Woogie - Piano roll QRS #7882," *Pianola & Jazzy Stuff YouTube Channel* (Oct. 28, 2010) https://www.youtube.com/watch?v=biZdjPI9akY.
[192] As James Foust reminds me, this is more accurately described as "high and low voltage memory cells that represent 1s and 0s."
[193] *Sorrell, et al. v. IMS Health Inc., et al.*
[194] *Information*, Oxford English Dictionary Online (2019) http://www.oed.com/viewdictionaryentry/Entry/95568.
[195] *Sorrell, et al. v. IMS Health Inc., et al.*
[196] *Universal City Studios, Inc. v. Reimerdes*, 82 F.Supp.2d. 211 (S.D.N.Y. 2000) aff'd 273 F.3d 429 (2d Cir. 2001).

> virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.[197]

While that rationale appears sensible, it also means that the the perpetrator of the expressive conduct (executing the code) will be treated under the law as equivalent to the person who originally authored speech that was later used in that conduct. This has significantly more complicated consequences than the expressive conduct cases upon which these lower court judges rely where the only "speaker" in question is the person actually performing the conduct.

To illustrate the absurdity of this approach, let's apply the reasoning of these lower court opinions to the facts in *Texas v. Johnson,*[198] an expressive conduct case that used the *Spence* and *O'Brien* analysis to strike down state laws banning flag burning. According to the analysis in *Corley*, laws affecting Betsy Ross's freedom to stitch the first American flag would be judged using the same intermediate scrutiny as laws affecting Johnson's freedom to burn said flag in front of the 1984 Republican National Convention. It may be that we should judge both laws strictly and protect both forms of expression. However, it is absurd to suggest that Ross, in her solitary act of patriotic creativity, carries any responsibility for Johnson's potentially dangerous street protest. Flags have several uses other than being burned, and Ross surely did not have this future public safety hazard in mind when she was sewing. Diminishing Ross's First Amendment rights (by qualifying them with intermediate rather than strict scrutiny review) simply because her flag was subsequently used in a burning "slides over questions of causation,"[199] to quote the judge in *Corley*.

This is not a stretched metaphor in the context of electronic cash and decentralized exchange software. Just like flags, that software is capable of at least as many non-subversive and legal uses as it is subversive or illegal uses. Similarly, the author of that software will likely have as little knowledge or awareness of what people are actually doing with her code as a flag designer will know of her flags. It is more logically consistent to say that a software developer produces speech (strongly protected under standards from *Roth* and *Sorell*), and that any person who runs that code is engaged in conduct (expressive or not), which is less protected under standards from *O'Brien* and *Spence*.

As some scholars have remarked, the expressive conduct cases may be an attempt "to reconcile the constitutional promise of expressive freedom with the practical need for governmental regulation."[200] Surely this is true, and people who blow up buildings in order to express political views should not enjoy First Amendment protection from prosecution. But is it right to deny protections to researchers whose chemical descriptions of dynamite made it, all other things being equal, much easier for someone those researchers had never met to commit an act of

---

[197] *Ibid*.
[198] 491 U.S. 397 (1989)
[199] *Id.*
[200] Genevieve Lakier, *The Invention of Low-Value Speech*, 128 Harv. L. Rev. 1 (2015) https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=11976&context=journal_articles.

terror? Is it legitimate to police harmful conduct by denying constitutional rights to persons who had no knowledge of the crime or the criminal, nor any intent to facilitate the crime?

Nonetheless, three out of four lower courts looking at the question of whether software is speech have confused the analysis between speech and conduct. This confusion could perhaps be reconciled by suggesting that the *Corley* line of thinking represents some new form of judge-made contributory liability for software developers; again, the judge in *Corley* found that "functionality is really 'a proxy for effects or harm.'"[201] If this is true, then it is an unheard of form of contributory liability that does not require knowledge of- or intent to aid the illegal act, and can even go so far as to abrogate otherwise protected constitutional rights. After all, if I publish code in a textbook that could potentially be used to violate copyright law (say it decrypts content protected with digital rights management tools) but nobody ever uses it, then there's no conduct and, presumably, it's now just speech and should be afforded the strongest First Amendment protection. If, however, one person uses my code to violate someone's copyright, then I no longer receive my full First Amendment rights (through no fault or action of my own). This would, we believe, be a rather unprecedented constitutional construct with no support from Supreme Court jurisprudence that we can find.

Indeed, the judge's reasoning sounds more like policymaking in response to a changed world than it does constitutional interpretation. Perhaps these policy changes *are* necessary now that "society increasingly depends upon technological means of controlling access to digital files and systems."[202] But that decision would be up to Congress[203] or the States,[204] and if it involved abrogating established constitutional rights it would require an amendment to the Constitution.[205] That's a far cry from tweaking the test for what types of expression qualify for protection under intermediate or strict scrutiny review.

This conduct-speech confusion may also be understood if one assumes that these courts have begun their analysis with the wrong case law. *Corley*, *Junger*, and *Karn* all begin with the premise that one must look to the line of cases dealing with expressive conduct in order to determine whether the code in question is protected at all (under either strict or intermediate scrutiny). This prejudices the later question: is the expression worthy of intermediate or strict scrutiny? Again, the Supreme Court found no need to inquire into whether buying and selling data about prescriptions was conduct in *Sorrell*, but rather started from the proposition that the data was speech because it was information.[206]

The only lower court to avoid confusing conduct and speech in the context of software, the district court in *Berstein*,[207] articulated the strangeness of the alternative approach with

---

[201] *Universal City Studios v. Corley*.
[202] *Ibid*.
[203] U.S. Const. Art. I Sec. I.
[204] U. S. Const. Amend. X.
[205] U.S. Const. Art. V.
[206] *Sorrell, et al. v. IMS Health Inc., et al.*
[207] *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt.

aplomb: "A computer program is so unlike flag burning and nude dancing that defendants' reliance on conduct cases is misplaced. It would be convoluted indeed to characterize [code for an encryption program] as conduct in order to determine how expressive it is when, at least formally, it appears to be speech."[208]

Putting this all together:

1. Electronic cash and decentralized exchange software is assuredly some kind of protected expression, either expressive conduct or mere speech.[209]
2. Expressive conduct receives weakened protection from regulation under intermediary scrutiny while plain speech receives robust protection under strict scrutiny review.[210]
3. Electronic cash and decentralized exchange software is published to express facts that advance human knowledge and allow us to conduct human affairs.[211]
4. This publication is entirely separate from the execution of the code by users when they make electronic cash transactions or conduct decentralized exchanges.[212]

Therefore, the publication of electronic cash and decentralized exchange software is protected as plain speech rather than expressive conduct, and it follows that laws governing its publication are subject to strict scrutiny review. In the final section we will look at how that review could unfold if regulators attempted to ban, require licensure for, or compel the inclusion of surveillance backdoors in the publication of electronic cash or decentralized exchange software.

C. Regulating Publication of Electronic Cash and Decentralized Exchange Software

First, an aside: We do not argue that electronic cash and decentralized exchange are wholly unregulated activities. Several activities, when performed using cryptocurrencies or smart contracts, are certainly regulated (*e.g.* accepting and transmitting cryptocurrency on behalf of others,[213] issuing new cryptocurrencies in a public sale with promises of future efforts to create profits,[214] trading cryptocurrency derivatives such as swaps or futures[215]) and several activities are simply illegal (laundering the proceeds of crime through cryptocurrency networks,[216]

---

[208] *Ibid*.
[209] *See supra* part IV. A. i. Computer Code Expresses Ideas for Political and Social Change, pp. 33-35.
[210] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45.
[211] *See supra* part IV. A. iii. Electronic Cash and Decentralized Exchange Software Are Protected Speech, pp. 37-39.
[212] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45; and part II. C. Electronic Cash and Decentralized Exchange are Powered by Software, pp. 15-17.
[213] US Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Guidance FIN-2013-G001 (Mar. 18, 2013) https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdfFincen Guidance
[214] *SEC v. Howey Co.*, 328 U.S. 293 (1946), https://supreme.justia.com/cases/federal/us/328/293/; Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies," *Coin Center* (Aug. 2018) https://coincenter.org/entry/framework-for-securities-regulation-of-cryptocurrencies.
[215] 7 U.S.C. ch. 1 §§ 4a-27f.
[216] 18 U.S.C. 1960.

sending cryptocurrencies to sanctioned persons[217]). Merely developing and publishing cryptocurrency software, however, is not at present an activity that triggers any regulation.

Electronic cash and decentralized exchange software is, to put it mildly, radically new. And like many new things, existing laws did not contemplate it, let alone prohibit or regulate it. A fundamental premise in Anglo-Saxon common law is *nulla poena sine lege* or "no penalty without law." As it stands, writing this type of software is not the subject of law and therefore it is, of course, allowed.

As discussed, the emergence of electronic cash and decentralized exchange will make transacting using cryptocurrencies more private and will, in many cases, eliminate the need to use BSA-regulated institutions in order to move from one cryptocurrency to another. If policymakers seek to subject these activities to greater financial surveillance, they will need to find new parties to regulate. As discussed earlier, regulating software developers as Financial Institutions under the BSA would result in a warrantless search and seizure violating the Fourth Amendment rights of the users of these networks. Without the ability to deputize these developers as agents of the U.S. financial surveillance regime, we can imagine calls to place restrictions on the publication and dissemination of electronic cash and decentralized exchange software.

To our knowledge, no policymaker has yet proposed a ban on, a licencing requirement for, or the compelled inclusion of a surveillance backdoor in the publication of electronic cash and decentralized exchange software. Nonetheless, should a law or regulation be put in place that attempts to do so, it would be unconstitutional under the First Amendment.

i. Banning Publication Would be Unconstitutional

Electronic cash and decentralized exchange software is constitutionally protected speech. Like all computer code, it should be understood properly as unadulterated speech and not as expressive conduct.[218] Supreme Court precedent provides no grounds for treating it as expressive conduct. Indeed, *Sorrell* advocates for pure speech treatment for data that is significantly less communicative.[219] Lower court opinions to the contrary engage in a dangerous process of judicial policymaking.[220] The emergence of electronic cash and decentralized exchange, as well as myriad other marvels of the still-recently connected world, may well necesitate new tradeoffs. But where those tradeoffs deal in policy they should be made by

---

[217] *See*: Office of Foreign Assets Control, "OFAC FAQs: Sanctions Compliance," *Department of Treasury*, https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx ("Yes, the obligations are the same [for virtual currency.] U.S. persons…must ensure that they block the property and interests in property of persons named on OFAC's SDN List or any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons.").
[218] *See supra* IV. A. Computer Code is Protected Speech, pp. 33-39.
[219] *Ibid*.
[220] *Id.*

Congress, and where those tradeoffs weaken constitutional rights they must be made through the process of constitutional amendment.

Regulations or laws that would ban the development or publication of electronic cash and decentralized exchange software would be prior restraints on speech. Prior restraint refers to restrictions on publication or distribution of speech made by government in advance of that publication or distribution. It can be contrasted with punishment-after-the-fact, wherein publication is allowed to proceed but may carry legal liability should the speech prove unprotected and unlawful. Regulations imposing prior restraint are usually unconstitutional and face extreme scrutiny. As the Supreme Court held in *Bantam Books v. Sullivan*, "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[221]

To rebut this presumption, the government faces strict scrutiny review of their policy. Again, this almost always means that the policy will be found unconstitutional. Nevertheless, we will run through the analysis here. Under strict scrutiny the government must prove that the ban is narrowly tailored to achieve a compelling interest.[222] A narrowly tailored policy must, in fact, advance the stated interest, it must not restrict a significant amount of speech unrelated to the interest, and there must not be a less restrictive means to achieve the interest.[223] The government may fail to show that its interest is compelling if the policy appears transparently incapable of achieving that interest,[224] and the government's interest cannot be an interest in privileging certain scientific and political ideas over others, even if this would, indeed, be compelling to government.[225]

Electronic cash and decentralized exchange software includes a broad class of published research and innovations with far-reaching potential to alter the way we organize society. Its developers and advocates genuinely believe that these scientific and engineering advances will, on net, improve the human condition and better guarantee human dignity and individual autonomy than alternative centralized and surveillance-accommodating tools for payments and exchange.[226]

A primary motivation behind the development of this technology is the global decline of cash transactions (which are inherently private and lacking in intermediaries).[227] This decline has been matched with the rise of powerful, private financial technology intermediaries that can systematically surveil their users and arbitrarily exclude them from economic life simply by closing their account. Such private surveillance and arbitrary power, argue electronic cash

---

[221] *Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963).
[222] Eugene Volokh, "Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny," 144 U. Pennsylvania L. Rev. 2417 (1997). *Available at* http://www2.law.ucla.edu/volokh/scrutiny.htm#12.
[223] *Ibid.*
[224] *Ibid.*
[225] *Ibid.*
[226] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.
[227] *Ibid.*

advocates, contravenes the rule of law. In nation states with weaker human rights guarantees, governments can and are actively partnering with these intermediaries to obtain greater control over their populations.[228] If cash disappears, advocates claim, only electronic cash and decentralized exchange technologies can serve as a safety valve against imminent payments-technology-enforced totalitarianism.[229]

One does not need to personally subscribe to these views in order to grasp the gravity of the constitutional law at hand. It is sufficient to believe that electronic cash and decentralized exchange software developers earnestly believe these views and publish their software to express them (rather than for some other cynical purpose). If this much is true, then bans on software publication wade dangerously into the territory of stifling a vibrant and consequential debate.[230]

Government may present its compelling interest for a ban as the prevention of crime, terrorism, or money laundering, rather than as an impermissible interest in stifling such debate. Other less restrictive policies, however, would both better advance that interest and burden substantially less speech. Banning publication would not prevent money launderers, terrorists, or criminals from using previously published or international versions of electronic cash or decentralized exchange software. The narrow way to address crime, terrorism, and money laundering is to more aggressively investigate, pursue, and apprehend money launders, terrorists, and criminals, not to ban dissemination of tools that criminals may use in their crimes, especially if those tools have non-criminal uses and if the developers have altruistic motivations and no knowledge of or intent to facilitate crime.

Courts have found that a policy's evident failure to effectively address the stated government interest is often indicative of there being some other undisclosed and impermissible government interest at play.[231] Again, a ban on electronic cash would self-evidently be an attempt to stifle the development of these tools and the beliefs that motivate that development. Such a ban thus privileges certain scientific and political ideas over others, and that cannot be an acceptable government interest.[232]

---

[228] *Id.*
[229] *Id*.
[230] *C.f.* Abrams v. United States, 250 U.S. 616, 630 (1919)(Holmes, J., dissenting) ("Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition…But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas… . The best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.")
[231] *See Florida Star v. B.J.F.*, 491 U.S. 524, 542 (1989) (Scalia, J., concurring in part and in the judgment); *Carey v. Brown*, 447 U.S. 455, 465 (1980).
[232] *See Carey*, 447 U.S. at 467; *see also* Consolidated Edison Co. v. Public Serv. Comm'n, 447 U.S. 530, 537-38 (1980).

Government interest aside, a ban would not qualify as a narrowly tailored policy. A narrowly tailored policy must not restrict a significant amount of speech unrelated to the government interest. Electronic cash and decentralized exchange promise a multitude of legitimate uses—not the least of them being a bulwark against totalitarian regimes.[233] Significant research, creativity, and non-criminal, non-money-laundering activities would be stopped or significantly chilled here in the U.S. if such a ban was to occur. Assuredly, some, if not most, electronic cash and decentralized exchange users are not engaged in crimes but simply want to try new technologies and protect their privacy and security. A ban would deprive this audience of the research and innovations provided by developers at least as much, if not more, than it would deny these tools to criminals, who would be less reticent to find and use a banned technology. The primary result would be a massive reduction in the freedom of law-abiding citizens. This is not narrow tailoring. As Justice Douglas wrote in the Fourth Amendment context, "I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."[234]

Lacking narrow tailoring and a convincingly compelling government interest, a blanket ban on the publication of electronic cash and decentralized exchange software would be unconstitutional.

ii. Licensing Regimes for Publication Would be Unconstitutional

A licensing regime is not a ban *per se*, and we can imagine a law or regulation that purported not to ban the publication of electronic cash and decentralized exchange software but merely license it. Perhaps the regulator would grant licenses only to software that included backdoors to enable surveillance of the resultant cryptocurrency networks, or perhaps the license would only be granted to certain 'qualified' developers as judged at regulator's discretion. These licensing schemes, however, would be unconstitutional for the same reasons that an out-and-out ban would be unconstitutional.

Speech licensing schemes, although they are not blanket bans, remain clear examples of regulations imposing prior restraint. As the Supreme Court held in *Lakewood v. Plain Dealer Publishing Co.*, "even if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion."[235]

The Supreme Court set out three factors for determining the constitutionality of licensing schemes in *Freedman v. Maryland*:

---

[233] *See* Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash; and Alex Gladstein, "Why Bitcoin Matters for Freedom" *Time* (December 28, 2018) http://time.com/5486673/bitcoin-venezuela-authoritarian/.
[234] *California Bankers Assn. v. Shultz*. (Douglas, J., dissenting).
[235] *Lakewood v. Plain Dealer Publ. Co.*, 486 U.S. 750 (1988) https://supreme.justia.com/cases/federal/us/486/750/.

1. Any restraint must be for a specified brief period of time,
2. There must be expeditious judicial review, and
3. The censor must bear the burden of going to court to suppress the speech in question and must bear the burden of proof.[236]

One of the lower court cases dealing with restrictions on distributing encryption code, *Bernstein v. Dep't of State*, analysed prior restraint and the constitutionality of a software publishing licencing scheme under the Arms Export Control Act (AECA) and its implementing regulations, the International Traffic in Arms Regulations (ITAR). The judge in *Bernstein* looked to the *Freedman* factors and found that the licensing scheme was unconstitutional.[237]

In *Bernstein*, the licensing scheme lacked any real standard or process of review apart from the discretion of the censor.[238] But even if there was a clear standard and process of review for our hypothetical scheme to limit publication of electronic cash and decentralized exchange software, conditioning approval on the presence of surveillance backdoors would be unconstitutional.

According to *Freedman*'s third factor, the censor bears the burden of going to court and defending every restraint on publication (*i.e.* denied license), and—in our hypothetical—each denial is predicated merely on the fact that the software does not incorporate a backdoor for identifying users. Therefore, each license denial and subsequent review should unfold as if it were a content-based ban on speech.

As discussed in the previous section, such a ban self-evidently seeks to privilege certain scientific and political ideas over others.[239] Each ban is a deliberate attempt to stymie valuable discussion concerning whether (both technologically and politically) we can and should have the ability to transact privately or exchange valuables over the internet without the need to rely

---

[236] *Freedman v. Maryland*, 380 U.S. 51 (1965) https://supreme.justia.com/cases/federal/us/380/51/.
[237] *Bernstein v. Dep't of State*, 176 F.3d 1132, 1136 (9th Cir.), *vacated for rehearing en banc*, 192 F.3d 1308 (1999), *available at* https://cr.yp.to/export/1996/1206-order.txt.
"The ITAR scheme, a paradigm of standardless discretion, fails on every count. This court finds nothing in the ITAR that places even minimal limits on the discretion of the licensor and hence nothing to alleviate the danger of arbitrary or discriminatory licensing decisions. Pt. 123, lays out an extensive list of requirements for those seeking a license but places no constraints on the ODTC in approving or denying a license. First, there is no limit to the time in which the ODTC must make a licensing decision. Second, not only does the ITAR not provide for judicial review of licensing decisions, prompt or otherwise, the AECA makes the initial designation of items as defense articles unreviewable. ... Finally, given there is no recourse for someone denied a license, there is no burden on the ODTC to go to court to justify the denial. Moreover, applications for licenses can be disapproved and approved licenses can be revoked, suspended or amended without prior notice in the interests of national security or whenever it "is otherwise advisable". ... While the court is mindful of the problems inherent in judicial review of ODTC licensing decisions regarding cryptographic software, both with respect to the sophistication of the technology and the potentially classified nature of the licensing considerations, there must still be some review available if the export controls on cryptographic software are to survive the presumption against prior restraints on speech." *Id.*
[238] *Id.*
[239] *See supra* IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech pp. 39-45.

on a trusted intermediary. There is nothing inherently illegal with making a private payment or trading a valuable asset, and the mere publication of information that enables or describes how one might enable those activities is, by its nature, an act of scientific and political discussion. As with a blanket ban, a licensing restriction would face strict scrutiny review and be found unconstitutional for its lack of a truly compelling interest and narrowly tailored approach to achieving that interest.

iii. Compelling Developers to Write Backdoors Would be Unconstitutional

Courts have long imposed a strong presumption against the constitutionality of any content-based ban on speech.[240] A similar presumption exists against laws that would compel persons to speak content they would otherwise avoid.[241] As Justice Jackson wrote in *West Virginia State Board of Education v. Barnette*, "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein."[242] *Barnette* concerned a state school board requirement that students must salute the flag at the start of each school day; the court found this requirement to be unconstitutionally compelled speech.

As with bans and licensing, however, the question of whether the expression being compelled is conduct or speech is often the decisive factor. In *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.*, for example, the court acknowledged as true "the principle that freedom of speech prohibits the government from telling people what they must say."[243] The Court, nonetheless, upheld an order that compelled schools to include military recruiters at job fairs. The Court reasoned that the order compelled schools to engage in conduct rather than the expression of a view. Schools would need to admit these military recruiters to their fairs alongside any other employers they invited, but they were not required to express any endorsement or approval of military employment. Thus, the order faced only intermediate scrutiny, and, as is typical with intermediate scrutiny in speech cases, it was upheld as constitutional.

Rumsfeld underscores the need to correctly analyze electronic cash and decentralized exchange software as speech rather than conduct, following Supreme Court precedent rather than the lower court opinions in *Corley*, *Junger*, and *Karn*, as discussed earlier.[244] Under such an analysis, a law compelling developers to publish software of a certain specification would face strict scrutiny and the state would bear the burden of proving that the law is narrowly tailored to achieve a compelling interest.

---

[240] *Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963).
[241] *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943) https://supreme.justia.com/cases/federal/us/319/624/.
[242] *Ibid.*
[243] *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47 (2006) https://supreme.justia.com/cases/federal/us/547/47/.
[244] *See supra* part IV. B. Strict vs. Intermediate Scrutiny for Regulation of Protected Speech, pp. 39-45.

An order that developers must write code that includes surveillance backdoors is tantamount to forcing developers to express a particular view in ongoing political and societal debates over privacy and security. Developers publish electronic cash and decentralized exchange software because they fervently wish to teach others *how* these private and person-to-person interactions are technologically possible and *why* they are essential to preserving human dignity and individual autonomy. Forcing such a developer to publish software that does the opposite—that compromises both the privacy of transacting parties with information-sharing and the autonomy of parties by reintroducing an intermediary—goes well beyond a simple order instructing a child to salute a flag. It is on par with forcing an academic to recant their previously published research and publish new, bogus research in its place or forcing a political organizer to condemn her constituency and form an opposition party. To paraphrase Justice Jackson, it prescribes what shall be orthodox in payments technology and forces developers to confess by word and act their faith therein.

An order to write such software is at least as coercive as an order that private parade organizers must include participants who would express beliefs not shared by the organizer[245] or an order that drivers must display the state motto on their license plate even if they find it objectionable.[246] In all of these cases, the court has consistently held that the order at issue is unconstitutional.[247]

As with a ban or license requirement, such an order would not be narrowly tailored—by forcing participants in a genuine debate to express views counter to their own, it would profoundly impact ongoing discussions about privacy and security, cause persons not engaged in any illegal act to use tools they otherwise would avoid, and introduce vulnerabilities into those tools that could be exploited by malicious persons other than the government.

As with a ban or license requirement, such an order would also fail to achieve the government interest at stake: uncompromised software would continue to be available to criminals via the internet, and privacy-protecting tools would be denied to those who are law abiding citizens. The government has a strong interest in preventing crime and money laundering. However, compelling hundreds or thousands of law-abiding developers of electronic cash and decentralized exchange software to affirm views they do not genuinely hold and publish

---

[245] *See, e.g.*, *Hurley v. Irish-American Gay, Lesbian, & Bisexual Group of Boston*, 515 U.S. 557 (1995).
[246] *See, e.g.*, *Wooley v. Maynard,* 430 U.S. 705 (1977).
[247] The compelled speech doctrine does have a narrow exemption that allows the state to order businesses to make "purely factual and uncontroversial information" disclosures about their products. This is why, for example, mandatory cigarette health warnings and nutrition fact labeling is constitutional. An order to publish software with surveillance backdoors is, however, expressive rather than factual and it would be anything if not uncontroversial. Indeed, even in the context of cigarettes, certain mandatory labeling efforts have been found non-factual and therefore unconstitutional. This is why American cigarette cartons lack the graphic photos of smoking-related disease that often can be found on cartons internationally. *See Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio*, 471 U.S. 626 (1985)

software they would never otherwise write is not a narrowly tailored approach to addressing those ills.

V. Conclusion

Electronic cash and decentralized exchange software development is essential for preserving human dignity and autonomy as the world moves increasingly toward fully intermediated payments technologies like Alipay or Wechat.[248] This report explained why anonymous electronic cash and decentralized exchange software is the endgame for all cryptocurrency networks, and how this evolution will result in much less publicly available information about cryptocurrency transactions. Postulating that this shift could trigger calls for more aggressive financial surveillance policies, we analyzed why two potential policy responses would be unconstitutional:

1. Regulating cryptocurrency software developers and individual users of that software under the Bank Secrecy Act, a federal surveillance statute, would be unconstitutional under the Fourth Amendment because it would be a warrantless search and seizure of information private to cryptocurrency users.
2. Furthermore, any law or regulation attempting to ban, require licensing for, or compel the altered publication (*e.g.* backdoors) of cryptocurrency software would be unconstitutional under First Amendment protections for speech.

We looked at over fifty years of U.S. case law, uncovering long-ignored questions about how the Fourth Amendment's warrant requirement can and cannot be reconciled with the Bank Secrecy Act, and why there is reason to doubt the full constitutionality of that law as currently applied. We investigated why lower court opinions from the Crypto Wars of the 1990s[249] are often misguided (even though many did protect encryption code as speech) and why recent Supreme Court case law provides a more robust shield against any attempt to regulate persons who are merely engaged in developing software.

There are many activities performed using electronic cash and decentralized exchange software that will be regulated, and some uses that will even be illegal. Nonetheless, an aggressive attempt to regulate software developers and individual users, as postulated in this report, would be a severe and unconstitutional overreach into our privacy and speech rights. Drawing that line will mean reduced tools for crime fighters and regulators, but that tradeoff has always been fundamental to American values and to open societies.

---

[248] *See*: Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash; and Alex Gladstein, "Why Bitcoin Matters for Freedom" *Time* (December 28, 2018) http://time.com/5486673/bitcoin-venezuela-authoritarian/.

[249] Specifically, *Universal City Studios, Inc. v. Corley* , *Junger v. Daley*, and *Karn v. US Dept. of State*. The Crypto Wars refers to broad debates over regulation of encryption in the 1990s. *See generally,* Paul Detrick, "How Government Lost the Crypto Wars (At Least for Now)" *Reason* (Mar. 1, 2018) https://reason.com/reasontv/2018/03/01/crypto-wars-how-encryption-went-mainstre.