NOTES

WAS I *SPEAKING* TO YOU?: PURELY FUNCTIONAL SOURCE CODE AS NONCOVERED SPEECH

MARK C. BENNETT*

This Note asks whether computer source code, when developed as a means to an end—as distinct from source code intended for third-party review—is covered speech under the First Amendment. I argue it is not. My argument has two parts. First, I describe case law treating First Amendment challenges to regulations of source code to demonstrate courts' failure to address the status of purely functional source code. Second, I describe how courts should address such a question, by referencing an array of theories used to explain the scope of the First Amendment. I conclude no theory alone or in combination with others justifies the constitutional coverage of purely functional source code. I thereby undermine a key constitutional argument by technology manufacturers contesting, in the context of criminal investigations, the government-compelled creation of software to circumvent encryption technologies.

 J.D., 2017, New York University School of Law. My thanks to Adam Winer and Chase Brennick, and the rest of the *New York University Law Review* editorial board, for their thoughtful comments during their review of this Note.

INTRODUCTION

Digital encryption uses software written in a language called source code[1] to convert plaintext messages into ciphertext (colloquially, "gobbledygook"[2]), which third parties cannot read without a sequence of numbers called a key.[3] This technology is neither new nor exotic. Today, nearly half of all Internet traffic is encrypted in some form,[4] and communications platforms—smart phones and messaging software—increasingly feature encryption architectures by default.[5]

---

[1] Source code is the version of a computer program as the programmer originally wrote it; it is not machine-readable. To perform a function, source code must be translated into object code (composed of strings of 1s and 0s), which is then compiled to create a file that may be understood by a computer. For a basic overview of these terms, see *Source Code Definition*, LINUX INFO. PROJECT (May 23, 2004), www.linfo.org/source_code.html, and *Object Code Definition*, LINUX INFO. PROJECT (Aug. 7, 2005), http://www.linfo.org/object_code.html.

[2] James B. Comey, Dir., FBI, Speech at the Center for the Study of American Democracy Biennial Conference: Expectations of Privacy: Balancing Liberty, Security, and Public Safety (Apr. 6, 2016), https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety.

[3] *See* JAMES A. LEWIS ET AL., CTR. FOR STRATEGIC & INT'L STUDIES, THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 1 (2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170203_Lewis_EffectOfEncryption_Web.pdf?Gqb5hXxckXykb3WAphuoVHrHfDTwuFkN (providing a layman's definition of digital encryption).

[4] *See* PETER SWIRE ET AL., INST. FOR INFO. SEC. & PRIVACY, ONLINE PRIVACY AND ISPS: ISP ACCESS TO CONSUMER DATA IS LIMITED AND OFTEN LESS THAN ACCESS BY OTHERS 41 (2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.may_2016.pdf (estimating approximately forty-nine percent of internet traffic used the secure version of the Hypertext Transfer Protocol (HTTPS)).

[5] *See* LEWIS ET AL., *supra* note 3, at 5–11 (summarizing applications of encryption in messaging applications, smartphones, and email). A report by the Center for Strategic and International Studies (CSIS) estimates forty-seven percent of all mobile devices in the United States are fully encrypted. *Id.* at iv. Take the Apple iPhone, for example, which claimed approximately forty-five percent of the domestic smartphone market share in the first quarter of 2017. *See comScore Reports January 2017 U.S. Smartphone Subscriber Market Share*, PR NEWSWIRE (Mar. 8, 2017, 11:02 AM), http://www.prnewswire.com/news-releases/comscore-reports-january-2017-us-smartphone-subscriber-market-share-300420345.html. Apple iPhones running iOS 8 or later versions are protected by an encryption key tied to the user's password known only by the user. *Legal Process Guidelines: Government & Law Enforcement Within the United States*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (last visited Sept. 25, 2017). At least

But what individuals gain in privacy, the public may lose in safety.[6] According to the Federal Bureau of Investigation (FBI), increased use of digital encryption has frustrated law enforcement's ability to intercept and access communications pursuant to lawful investigations.[7] Government officials claim this lack of access to encrypted communication limits their ability to prosecute criminal activity and prevent terrorist attacks.[8] Of the 3000 devices the FBI seized between October 2015 and April 2016, about thirteen percent were inaccessible because of their security features.[9] Local officials have encountered similar difficulties. In the Manhattan District Attorney's Office, for example, 423 encrypted Apple devices lawfully seized in relation to cybercrime, drug, and violent offenses remain unopened.[10]

---

ninety-five percent of iPhones operate with iOS 9 or 10. *Support*, APPLE, https://developer.apple.com/support/app-store/ (last visited Sept. 25, 2017).

[6] *See* James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead*, LAWFARE (Feb. 21, 2016, 9:03 PM), https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead ("[W]e have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety."). *But see* LEWIS ET AL., *supra* note 3, at 12–16 (suggesting the purported tradeoff between privacy and safety lacks empirical support).

[7] *See generally Going Dark*, FBI, https://www.fbi.gov/services/operational-technology/going-dark (last visited Sept. 25, 2017) (describing the "Going Dark" problem).

[8] In congressional testimony, former FBI Director James Comey and former Acting Attorney General Sally Yates put it bluntly: "When changes in technology hinder law enforcement[ ] . . . we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root out the child predators hiding in the shadows of the Internet . . . ." *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 3–4 (2015) (joint statement of James B. Comey, Dir., FBI & Sally Quillian Yates, Deputy Att'y Gen. of the United States), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf.

[9] *See Deciphering the Debate over Encryption: Industry and Law Enforcement Perspectives: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce*, 114th Cong. 103 (2016) (statement of Amy Hess, Executive Assistant Director for Science and Technology, FBI), http://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Transcript-20160419.pdf (stating in the first six months of the 2015–2016 fiscal year, the FBI could not access thirteen percent of seized encrypted devices) [hereinafter *Deciphering the Debate over Encryption*]; LEWIS ET AL., *supra* note 3, at 14 (stating the FBI seized over 3000 devices in the same period).

[10] DIST. ATTORNEY OF N.Y. CTY., REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 8 (2016), http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; *see also Deciphering the Debate over Encryption*, *supra* note 9, at 103–04 (describing New York City and Indiana State officials' experiences with encrypted devices). The Los Angeles Police Department reported 300 unopened encrypted devices; Charlotte-Mecklenburg, North Carolina reported 160; Suffolk County, Massachusetts reported 151; the Los Angeles County Sherriff reported

Opponents of strong default encryption point to myriad instances where law enforcement's inability to access devices discovered at crime scenes has stymied investigations.[11] The December 2015 San Bernardino terrorist attack is a prime example.[12] After the shooting, officials sought data encrypted on one suspect's iPhone.[13] When the FBI's "brute force" method of unlocking the device failed,[14] it sued to compel Apple to create software to override the phone's security features, which would erase the phone's data after a series of unsuccessful attempts to unlock it.[15] Though the FBI eventually gained access to the device with an outside contractor's assistance—thereby mooting the legal dispute[16]—the policy debate on the propriety of the FBI's legal strategy remains.

150; Austin, Texas reported 45; and the Chicago Regional Computer Forensic Laboratory reported 30. LEWIS ET AL., *supra* note 3, at 15.

[11] *See* DIST. ATTORNEY OF N.Y. CTY., *supra* note 10, at 10–11 (listing examples of criminal cases nationwide involving encrypted iPhones). Recently, Manhattan district attorney Cyrus Vance coauthored an editorial with international law enforcement officials saying, "Why should we permit criminal activity to thrive in a medium unavailable to law enforcement? To investigate these cases without smartphone data is to proceed with one hand tied behind our backs." Cyrus R. Vance, Jr. et al., *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

[12] *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.f5e233738134. The attack killed fourteen people and injured twenty-two.

[13] *Id.*

[14] A "brute force" method involves using a computer to input all possible passwords until it guesses the correct one. *See* Mike Isaac, *Explaining Apple's Fight with the F.B.I.*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html?_r=0.

[15] Vindu Goel, *A Brief Explanation of Apple's Showdown with the U.S. Government*, N.Y. TIMES (Feb. 26, 2016), https://www.nytimes.com/2016/02/27/technology/a-brief-explanation-of-apples-showdown-with-the-us-government.html. A California federal court granted the FBI's request, allowing Apple five days to answer if the order would be unreasonably burdensome. *In re* the Search of an Apple iPhone Seized During the Execution of a Warrant, No. ED 15-0451M at 3 (C.D. Cal. Feb. 16, 2016) [hereinafter Order Compelling Apple, Inc.] (compelling Apple, Inc. to assist agents in search).

[16] After the Central District of California's order to compel Apple's assistance in the matter, Order Compelling Apple, Inc., at 3, Apple promptly moved to vacate the order. Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant, No. CM 16-10 (SP) (C.D. Cal. Feb. 25, 2016), https://www.eff.org/document/apple-fbi-all-writs-apple-motion-vacate-and-declarations. The government accessed the phone late in March 2016, after argument on Apple's motion to vacate, but before the court rendered a final judgment. *See* Katie Bo Williams & Cory Bennett, *Apple, FBI Fight Goes to Court on Tuesday*, THE HILL (Mar. 21, 2016, 5:49 PM), http://thehill.com/policy/cybersecurity/273812-apple-fbi-fight-goes-to-court-on-tuesday (stating oral argument was scheduled to be held on March 22); Joel Rubin et al., *FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle with*

Critics of the Bureau's position—that law enforcement and national security interests justify circumvention of encryption—primarily invoke three substantive arguments.[17] First is the privacy argument,[18] which argues obtaining a workaround of Apple's encryption in one investigation undermines the security of not only the suspect, but the security of all customers relative to law enforcement and to others savvy enough to use a "backdoor."[19] Second is the due process argument, which suggests compelled decryption violates an individual's privilege against self-incrimination.[20] Third is the First Amendment argument, which asserts that when a court commands a

Apple, for Now, L.A. TIMES (Mar. 28, 2016, 10:39 PM), http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html (stating the government dropped its suit after obtaining access with the aid of an outside contractor).

[17] These do not include procedural arguments questioning the appropriateness of the FBI using the All Writs Acts to compel manufacturer assistance in these cases. *E.g.*, Apple Inc.'s Motion to Vacate, *supra* note 16, at 14–32; *see also In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court at 1, No. 15-MC-1902 (JO) (E.D.N.Y. Feb. 29, 2016), https://epic.org/amicus/crypto/apple/Orenstein-Order-Apple-iPhone-02292016.pdf (denying an order, in a separate and unrelated criminal case, to require Apple to bypass security features on an Apple device for lack of basis in the All Writs Act).

[18] *See generally, e.g.*, Maxel Moreland, *Apple Inc. and the FBI: Balancing Fourth Amendment Privacy Concerns Against Societal Safety Concerns in the Digital Age*, U. CIN. L. REV. ONLINE (June 17, 2016), https://uclawreview.org/2016/06/17/apple-inc-and-the-fbi-balancing-4th-amendment-privacy-concerns-against-societal-safety-concerns-in-the-digital-age/ ("Requiring Apple to develop software that breaks the iOS security would continue the degradation of technological privacy.").

[19] *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ ("The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key . . . .").

[20] *See generally* Brief for the American Civil Liberties Union Foundation of Massachusetts et al. as Amici Curiae in Support of the Defendant-Appellee, Commonwealth v. Gelfgatt, 468 Mass. 512 (2014) (No. 11358), https://www.eff.org/document/effaclu-gelfgatt-amicus-brief (arguing compelled decryption violates the Fifth Amendment privilege against self-incrimination); Benjamin Folkinshteyn, *A Witness Against Himself: A Case for Strong Legal Protection of Encryption*, 30 SANTA CLARA HIGH TECH. L.J. 375 (2014) (noting the tension between the Fifth Amendment and compelled disclosure of encrypted information); *cf.* Dan Terzian, *The Micro-Hornbook on the Fifth Amendment and Encryption*, 104 GEO. L.J. ONLINE 168 (2016) (arguing compelled decryption may be permissible under certain circumstances); Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand over Passwords*, 30 BERKELEY TECH. L.J. 1, 24–30 (2015) (arguing that while compelled disclosure of encryption passwords implicates the privilege against self-incrimination, the Fifth Amendment provides inadequate defense against such compulsion).

manufacturer to write software to neutralize security features, the court unconstitutionally compels speech in the form of software.[21]

Whatever the merits of the first two arguments, the third rests on a doctrinally and theoretically problematic assumption. Specifically, it depends on the premise that the First Amendment covers all computer code.[22] This assumption relies, in turn, on a spate of cases, now more than a decade old, interpreting statutory restrictions on the distribution of encryption technologies, cases that do not agree on whether or why encryption source code falls under the Constitution's aegis.[23]

Neither the Supreme Court nor any court since 2004 has addressed the constitutional status of encryption source code directly, and no court has ever addressed the constitutional status of code created specifically to circumvent encryption pursuant to a criminal investigation. But after a decade of rising tensions between private interests not apparent in previous litigation and law enforcement's focus on the "going dark" problem, determining the constitutional status of these types of source code has become more urgent.[24]

This Note resolves the case law's unresponsiveness to the present technological setting by asking one question: Is purely functional source code speech covered by the First Amendment? By purely functional source code, I mean code not designed to participate in scientific dialogue, education, or other interpersonal communicative activities. Created by a programmer under conditions of secrecy, this type of code communicates only to a computer to perform a mechanical function, like converting plaintext to ciphertext,[25] circumventing

---

[21] Apple made this argument in its appeal of the California court's order to assist the FBI in the San Bernardino investigation. Apple Inc.'s Motion to Vacate, *supra* note 16, at 32–34; *see also* Steve Lohr, *Analyzing Apple's Argument that First Amendment Applies to Its Code*, N.Y. TIMES (Feb. 25, 2016), https://www.nytimes.com/2016/02/26/technology/in-apple-case-addressing-the-legal-status-of-code.html (describing a viewpoint discrimination claim related to Apple's appeal of the court order).

[22] *See* Apple Inc.'s Motion to Vacate, *supra* note 16, at 32 ("[C]omputer code is treated as speech within the meaning of the First Amendment.").

[23] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1099–1100 (N.D. Cal. 2004); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002); Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996). Apple cited each of these cases in its litigation against the government. Apple Inc.'s Motion to Vacate, *supra* note 16, at 32. I discuss these cases in depth in Part I.

[24] *See supra* notes 4–5 (noting the rising prevalence of encryption technologies); *see also supra* notes 7–10 (noting problems encryption technologies pose to law enforcement).

[25] *See supra* notes 1–5 and accompanying text (describing encryption source code).

encryption architectures,[26] or coordinating actions among parts of a computer.[27] I leave to one side what I term "expressive source code," or source code designed for or used as part of an exchange of ideas among programmers for the advancement of computer science or for the instruction of code writers, for example.[28]

I argue purely functional source code is not covered speech.[29] Nor should it be so considered under an array of theories used to explain the scope of First Amendment coverage.[30] By refuting the prevailing assumption the First Amendment covers source code generally,[31] I undermine the critical premise supporting the manufacturer's refusal to create purely functional source code to circumvent encryption architectures in mobile devices.[32] The upshot: An encryp-

---

[26] *See supra* note 15 and accompanying text (describing the type of encryption-circumvention software sought in the Apple litigation).

[27] Examples of this type of software include operating systems. *See* FRANCIS M. ALLEGRA & DANIEL B. GARRIE, PLUGGED IN: GUIDEBOOK TO SOFTWARE AND THE LAW § 2.5 (2015) ("The operating system platform is both a resource allocator and a control program. As a resource allocator, an operating system manages the CPU time, memory space, [and] file-storage space . . . . As a control program, an operating system controls the execution of programs to prevent errors and ensure the machine operates properly." (citations omitted)).

[28] Examples of this type of code include those at issue in the export restrictions litigation. *See infra* Section I.A. In each case, the code at issue was designed to serve an academic purpose. *See id.* I propose a counter to my own premise: Could not functional source code, belonging to, say, Apple, nonetheless become expressive source code if, after an inadvertent disclosure, it becomes subject of public controversy? Now, an answer: Yes. But when appropriated by a third party, such code becomes the expression of the third party, not of Apple.

[29] I used the term coverage—not protection—deliberately. My argument is not that government regulations of source code performing a purely functional purpose (for example, circumvention software at issue in the Apple litigation) regulate unprotected speech (akin to obscenity, for example), thereby invoking a lesser form of judicial scrutiny than protected speech (for example, political speech). My argument is that such regulations do not invoke judicial scrutiny at all because they do not regulate speech within the meaning of the First Amendment. For a fuller discussion on the distinction between First Amendment coverage and protection, see, for example, Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1769–74 (2004).

[30] *See infra* Section II.A (discussing the marketplace-of-ideas rationale, the democratic self-government theory, the individual autonomy rationale, and a novel social context theory).

[31] *See infra* Sections I.A–B (explaining how a majority of courts that have approached the similar question of publicly available encryption source code have deemed such code speech covered by the First Amendment).

[32] Apple contested the government's demand to create nonencryption source code to circumvent the encryption architectures within a smartphone on the basis that computer source code is speech, citing exclusively to cases discussing encryption source code. Apple Inc.'s Motion to Vacate, *supra* note 16, at 32. By undermining the premise that these cases support—or should support—the broad statement that computer code is speech, I refute Apple's conclusion that the government seeks to compel speech by the creation of circumvention software.

tion technology manufacturer may not invoke a First Amendment defense when refusing to create software designed to circumvent device encryption pursuant to a criminal investigation.[33]

* * *

This Note has two Parts. Part I is doctrinal. It outlines how courts *have* addressed the constitutional status of source code in the two lines of cases to confront this question directly. It concludes that courts' finding that source code used or capable of use in the scientific exchange of ideas is covered by the First Amendment does not lead necessarily to the conclusion that *purely functional* source code deserves similar constitutional status. Indeed, it suggests such source code is distinct from expressive code for the purposes of the First Amendment. Part II is normative. It suggests how courts *should* address the constitutional status of source code. In doing so, I contest the relevance to the problem of purely functional source code of several theories used to delimit First Amendment coverage: the marketplace-of-ideas rationale, the democratic self-governance rationale, the individual autonomy rationale, and a social-context–based rationale proposed by Robert Post.[34] I also challenge a mode of analysis by which First Amendment coverage may be discerned by governmental motives for regulation.[35] I conclude purely functional source code—code used purely as a means to an end—does not merit constitutional coverage under any of these theories.

I
How Courts Have Assessed the Constitutional Status of Source Code

Disputes implicating the constitutional status of source code primarily arose under two statutory regimes: the export control system authorized by the Export Administration Act, and the Digital Millennium Copyright Act. This Part interrogates the cases pertaining to each separately to draw four conclusions: First, some courts have seemed reluctant to explain the constitutional status of source code by assuming, but without deciding, such code merits First Amendment protection, reflecting in part the lack of a common First Amendment theory with which to approach the problem. Second, and relatedly,

[33] *See supra* note 22 and accompanying text (describing Apple's First Amendment argument, which relied on the problematic assumption that the First Amendment covers all computer code).

[34] *See infra* Section II.A.

[35] *See infra* Section II.B.

courts that have addressed the question did so in very different ways: Of the five courts to recognize source code as deserving some constitutional protection, only two opinions carrying precedential effect offer theories of free speech to explain their holding. One holds that coverage extends to all forms of source code;[36] the other, in dicta, would decline a categorical approach.[37] Third, notwithstanding the inconsistency in these cases' approach to source code, they largely recognize either explicitly or implicitly a legal difference between code deemed speech and code performing a purely mechanical function. Fourth, no court has addressed the precise issue this Note discusses—the status of purely functional source code used only as a means to an end. Together, these four conclusions indicate when a litigation finally presents such a question, the adjudicating court will need to look elsewhere for guidance in approaching the question of the constitutional status of purely functional code.

A. Export Restrictions

The Export Administration Act authorizes the President to impose export controls on sensitive commodities having civilian and military applications (dual-use technologies).[38] Pursuant to this authority, the Department of Commerce enforces the Export Administration Regulations, which include a description of items subject to licensing requirements.[39] Generally, exporters may export material without a license provided they comply with the regulations' guidelines.[40] In contrast, encryption technologies must be submitted for review before exporting.[41] An adverse ruling prohibits the export

---

[36] *See infra* Section I.A.2 (discussing Junger v. Daley, 209 F.3d 481 (6th Cir. 2000)).

[37] *See infra* Section I.B.2 (discussing Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)); *see also* notes 99–102 and accompanying text (comparing *Junger* and *Corley*).

[38] 50 U.S.C. § 2405(a)(1) (2012).

[39] 15 C.F.R. §§ 730–74 (2017). Specifically, the Bureau of Industry and Security administers these regulations. *See Regulations*, BUREAU INDUSTRY & SECURITY, U.S. DEP'T COM., https://www.bis.doc.gov/index.php/regulations (last updated July 7, 2017). Prior to 1996, the State Department had jurisdiction over nonmilitary encryption technologies, administering a similar regime under the International Traffic in Arms Regulation. *See* Exec. Order No. 13,026, 3 C.F.R. §§ 228, 229 (1996–1997) (transferring authority of export controls of encryption products from the State Department to the Commerce Department); 22 C.F.R. §§ 120.1(a), 124.15 (2014) (implementing the International Traffic in Arms Regulation and assigning the regulation of encryption technology export to the State Department).

[40] *See* 15 C.F.R. §§ 732.1–6 (describing steps for determining whether the regulations require a license application).

[41] 15 C.F.R. § 742.15 (describing conditions under which encryption technologies require an export license); *see* Jeffrey Richardson, *Is Your Software Transmission Subject to U.S. Export Controls Under the EAR?*, MILLER CANFIELD (May 3, 2013), https://

of that technology.[42] The following three cases result from denials of applications for export licenses. Each emphasizes the significance of the expressiveness of code in determinations of its First Amendment status. In doing so, each indicates, either expressly or implicitly, code without expressive intent may be subject to a separate analysis.

1. Karn v. U.S. Department of State

In *Karn v. U.S. Department of State*, the District Court for the District of Columbia rejected a software engineer's claim that designation of a diskette containing encryption source code as a defense article subject to export restriction constituted an unconstitutional restraint on speech.[43] In doing so, the court accepted as a threshold matter—but without explanation—plaintiff's argument that the First Amendment covered the contents of the diskette.[44] However, the diskette contained not only source code, but comments embedded within the code intended to serve an instructive purpose.[45] Without these comments, the court may have decided the threshold issue differently. The court said in a footnote: "The Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment. Source codes are merely a means of commanding a computer to perform a function."[46]

In effect, the court distinguished between categories of coded language: one intended for a person (covered by the First Amendment, albeit for reasons unstated by the court), the other for a computer (perhaps not covered); one expressive, the other purely functional. In doing so, the court raised, for the first time, whether the functionality

---

www.millercanfield.com/resources-alerts-845.html ("A key determinant as to the level of control for software under the EAR is the presence of data encryption.").

42 15 C.F.R. § 736.2(b)(1).

43 925 F. Supp. 1, 3 (D.D.C. 1996). Applying intermediate scrutiny to what it deemed a content-neutral regulation, the court found the statute fell within government's power to control the export of defense articles, advanced the significant government interest of preventing the proliferation of cryptographic products, and was narrowly tailored to that end. *Id.* at 11–12. For procedural history not offered by the opinion, see Brief of the Appellant Philip R. Karn, Jr. at 2–3, Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996) (No. 96-5121).

44 *Karn*, 925 F. Supp. at 9 ("[F]or the purpose of addressing the dispositive issue whether the regulation is justified and permissible, the Court will assume that the protection of the First Amendment extends to the source code . . . .").

45 *Id.* (describing plaintiff's argument that comments are "useful only to a human and . . . ignored by a computer" and which "teach humans how to speak in code").

46 *Id.* at 9 n.19.

of source code determines its constitutional status.[47] For now, I note only that the court left the question unanswered.[48]

2. Junger v. Daley

In *Junger v. Daley*, the Northern District of Ohio rejected a law professor's claim that export regulations administered by the Department of Commerce work an unconstitutional prior restraint,[49] because the export of encryption software did not qualify as speech under the First Amendment.[50] The court offered two observations that begin to answer the question *Karn* raised only in passing, while also challenging that court's assumption of constitutional coverage for encryption source code. First, the court recognized encryption software's inherent functionality predominates over its expressive content.[51] Second, it rejected the argument that communication expressed in language necessarily merits protection: "[W]hat determines whether the First Amendment protects something is whether it expresses ideas."[52] However, it sidestepped any finding that encryption source code was not covered speech, instead noting that the *act* of exporting such material, though occasionally expressive when done to communicate ideas about cryptography, is subject to regulation.[53]

---

[47] I emphasize that *Karn* did not hold specifically such a distinction is dispositive, for the court did not decide the question of source code's constitutional status. Note *Karn*'s distinction among different types of source code evokes the Supreme Court's early explanation of its approach to technological innovation in *Red Lion Broadcasting Co. v. FCC*. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 386 (1969) ("[D]ifferences in the characteristics of new media justify differences in the First Amendment standards applied to them.").

[48] As later sections indicate, not all courts were as indecisive in describing this distinction's importance. *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001) (suggesting speech communicated to a computer by a programmer is never covered by the Constitution (citing Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000))).

[49] A prior restraint is a rule operating to forbid expression before it happens. 2 SMOLLA & NIMMER ON FREEDOM OF SPEECH § 15:1 (2017).

[50] 8 F. Supp. 2d 708, 715–19 (N.D. Ohio 1998), *rev'd*, 209 F.3d 481 (6th Cir. 2000). Junger had sought—and was denied permission—to publish source code online because the publication qualified as an export under the Export Administration Regulations. *Id.* at 714. Plaintiff had four claims in addition to a prior restraint claim: statutory overbreadth and vagueness, content discrimination, infringement of academic freedom and freedom of association, and violation of the separation of powers. *Id.* at 711–12. The court rejected each. *Id.* at 723–24.

[51] *Id.* at 716 ("Among computer software programs, encryption software is especially functional rather than expressive. . . . More than describing encryption, the software carries out the function of encryption.").

[52] *Id.* (citing Roth v. United States, 354 U.S. 476, 484–85 (1957)).

[53] *Id.* at 719 ("[T]he Court finds that the Export Regulations are not narrowly directed at expressive conduct, and therefore not a prior restraint . . . .").

On appeal in 2000, the Sixth Circuit reversed the District Court's ruling, finding that the First Amendment covered computer source code because "it is an expressive means for the exchange of information and ideas about computer programming."[54] In doing so, the Court of Appeals did not address code specifically created for practical use without academic input, "final-draft code" resulting from peer-to-peer review,[55] or "bare code"—code without comments—that *Karn* mentioned[56] without analysis.[57] Indeed, under the Sixth Circuit's premise, according to which language routinely used for expressive purposes is speech, code having no expressive purpose, except for communication with a computer, may fall outside the First Amendment's scope.

3. Bernstein v. United States Department of Justice

The first definitive answer to the question of the constitutional status of encryption source code came from the Ninth Circuit in 1999: "[E]ncryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine."[58] This conclusion rests on the assumption that source code facilitates the precise expression of algorithmic ideas otherwise difficult to achieve among cryptographers.[59]

The facts of *Bernstein* limited the court's analysis to source code used in the academic context, however. As in *Junger*, the plaintiff sought a prepublication license of encryption material for use within the scientific community.[60] The court's discussion of source code

---

[54] Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000).

[55] Moritz Beller et al., Modern Code Reviews in Open-Source Projects: Which Problems Do They Fix? 2 (May 2014) (unpublished manuscript), http://sback.it/publications/msr2014.pdf (defining peer code review as a project intended to suss out errors from a draft submitted by an author).

[56] *See* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) ("The Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment.").

[57] The Sixth Circuit phrased its holding as follows: "*Because 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." *Junger*, 209 F.3d at 485 (emphasis added).

[58] Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.) (finding the prepublication licensing requirement under the Export Administration Regulation constitutes a prior restraint), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

[59] *Id.* ("By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve.").

[60] *Id.* at 1136. The State Department had declared a computer program and corresponding instructions restricted; the Department did not restrict a paper containing related mathematical analysis, however. *Id.* at n.2.

focused almost exclusively on its use among cryptographers for the purpose of peer-to-peer review.[61] Like *Junger*, *Bernstein* did not provide a basis on which to assess the constitutional status of all source code.[62] Worse, the Ninth Circuit withdrew the *Bernstein* decision,[63] rendering the opinion without precedential effect.

* * *

Notice: None of these cases settle the question of whether encryption source code used only as a means of data encryption (i.e., purely functional source code) merits coverage under the First Amendment. Nonetheless, they do suggest a distinction between purely functional source code and expressive source code. *Karn* noted the relevance of comments in code;[64] *Bernstein* limited its analysis to code as used in cryptography;[65] and *Junger* premised its broad holding on an assumption about the expressiveness of code.[66]

In the next Section, I demonstrate how a parallel line of cases similarly failed to resolve definitively the issue of the constitutional status of source code used purely as a means to an end.

B. Digital Millennium Copyright Act

To protect against unauthorized distribution of its DVDs, the film industry used an access-control encryption system called the Content Scramble System (CSS).[67] Until programmers learned to decrypt data themselves with a decryption program called DeCSS, only CSS-licensed players enabled viewing of licensed DVDs.[68] In support of the content-production industry's efforts to protect its copyrightable content, Congress passed the Digital Millennium Copyright Act (DMCA), criminalizing the circumvention of technological measures,

---

[61] *See id.* at 1141 (concluding "encryption software, in its source code form and as employed by those in the field of cryptography" merits constitutional coverage).

[62] *See supra* notes 55–57 and accompanying text (discussing the types of source code that were not addressed by the *Junger* court's holding).

[63] Bernstein v. U.S. Dep't of Justice, 192 F.3d 1308 (9th Cir. 1999). A rehearing never occurred.

[64] *See* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) (noting that the ruling does not address source codes without the comments).

[65] *Bernstein*, 176 F.3d at 1141.

[66] *See* Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) (noting that computer code is a method of sharing information and ideas about computer programming).

[67] *See* Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263, 276 (2002) (describing how CSS thwarts the practice of "ripping" content from digital storage, including CDs and DVDs).

[68] *See id.* at 291 (describing the creation of DeCSS, a program capable of "ripping" DVDs).

like CSS that effectively control access to a copyrighted work.[69] The following cases arise from disputes challenging the constitutionality of the DMCA's anticircumvention provisions and constitute the second series of litigations implicating the constitutional status of source code.

1. Universal City Studios, Inc. v. Reimerdes

In *Universal City Studios, Inc. v. Reimerdes*, the Southern District of New York issued a preliminary injunction barring online distribution of the DeCSS program.[70] Defendants disputed the constitutionality of the DMCA on the basis that it worked an unconstitutional prior restraint by prohibiting the dissemination of a computer program to the public.[71] Noting that the district court in *Junger* and *Bernstein* had come to different conclusions on the question of encryption software's First Amendment status,[72] the court declined to rule definitively on the issue.[73] However, the court did suggest a preference for the lower court's opinion in *Junger* when it observed that the expressive aspect of DeCSS source code "appears to be minimal when compared to its functional component. . . . It arguably 'is best treated as a virtual machine . . . .'"[74] The court further said, "The fact that there may be some expressive content in the code should not obscure the fact that its predominant character is no more expressive than an automobile ignition key."[75] Therefore, *Reimerdes* continues

[69] 17 U.S.C. §§ 1201, 1204 (2012). For background on the law's enactment, see HOWARD COBLE, WIPO COPYRIGHT TREATIES IMPLEMENTATION AND ON–LINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION, H.R. REP. NO. 105-551, pt. 1, at 10 (1998) ("[T]he U.S. must make it unlawful to defeat technological protections used by copyright owners to protect their works.").

[70] 82 F. Supp. 2d 211 (S.D.N.Y. 2000). Defendants owned a website instructing viewers how to use DeCSS. *Id.* at 214–15.

[71] *Id*. at 220–26. Specifically, defendants asserted the DMCA worked an invalid prior restraint on their speech. *Id.* at 224; *see* 2 SMOLLA & NIMMER, *supra* note 49 (defining prior restraint).

[72] The Sixth Circuit only reversed the District Court's decision in *Junger* two months after the District Court decided *Reimerdes*.

[73] 82 F. Supp. 2d at 219–20 ("[T]his Court assumes for purpose of this motion, although it does not decide, that even the executable code is sufficiently expressive to merit some constitutional protection."). Note that no court had recognized that executable code, or object code, designed for encryption is constitutionally protected speech, making *Reimerdes* anomalous in this regard. Recall that object code is machine-readable code (as distinct from source code, which cannot be understood by a computer). See *supra* note 1 for a brief definition of these terms.

[74] 82 F. Supp. 2d at 222 (quoting Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 236–37 (1998)).

[75] *Id.* at 226. Note the contrast with *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1142 (9th Cir.) ("[W]e reject the notion that the admixture of functionality necessarily puts

an argument begun in *Junger* that functionality may determine the constitutional status of encryption source code.

2. Universal City Studios, Inc. v. Corley

Under similar facts as *Reimerdes*, the Second Circuit in *Universal City Studios, Inc. v. Corley* upheld an injunction instituted by the lower court barring a website owner from distributing DeCSS.[76] The court rejected defendant's claim that the DMCA unconstitutionally restricted speech.[77] Unlike *Reimerdes*, though, it recognized source code as speech, in part for its expressive applications.[78] Like the court in *Bernstein*, the Second Circuit emphasized that programmers use code to communicate with each other.

But this argument seemingly conflicts with the Second Circuit's previous holding in *Commodity Futures Trading Commission v. Vartuli*. There, the Second Circuit observed that "none of the reasons for which speech is thought to require protection . . . beyond that accorded to non-speech behavior" counseled in favor of treating notifications by a software program to users when to buy or sell futures contracts as "constitutionally protected speech."[79] This conclusion relied on the argument, acknowledged by *Corley*, that a system using words as triggers and humans as conduits does not materially differ from a system that uses commands as triggers and semiconductors as conduits (essentially the function of software on a computer).[80] The

---

expression beyond the protections of the Constitution."), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

[76] 273 F.3d 429, 434–35 (2d Cir. 2001). Defendant had posted a copy of DeCSS to his website. *Id.* at 439.

[77] The court applied intermediate scrutiny to the statute and found the statute furthered the substantial governmental interest of preventing unauthorized access to encrypted copyrighted material, and the statute did not burden substantially more speech than necessary to further that interest. *Id.* at 453–60.

[78] *Id.* at 448 ("[P]rogrammers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars . . . .").

[79] Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000). *Corley* characterized *Vartuli*'s argument more starkly, stating the previous decision found notifications by software to users to be "devoid of any constitutionally protected speech." *Corley*, 273 F.3d at 449 (citing *Vartuli*, 228 F.3d at 112).

[80] "From a First Amendment perspective, [the program] did not materially differ from a system in which Recurrence's signals electronically triggered trades . . . [T]he fact that the system used words as triggers and a human being as a conduit, rather than programming commands as triggers and semiconductors as a conduit, appears . . . irrelevant . . . ." *Vartuli*, 228 F.3d at 111. *See also Corley*, 273 F.3d at 449 n.23 ("*Vartuli* reasoned that the interaction between 'programming commands as triggers and semiconductors as a conduit,' even though communication, is not 'speech' within the meaning of the First Amendment and that the communication between [software] and a customer using it as intended was

implication is this: When a programmer communicates with a computer by way of a software program, the First Amendment does not apply to that communication.[81]

3. United States v. Elcom Ltd.

In *United States v. Elcom Ltd.*, the Northern District of California denied defendant's motion to dismiss an indictment for violating the DMCA for the distribution of software designed to remove access-control features of electronic books.[82] Though the court found the DMCA to be a lawful content-neutral restriction on speech, it recognized "computer code"—even object code—to be speech within the meaning of the First Amendment.[83] For support, the court cited a single case holding video game software copyrightable.[84] If such software is copyrightable, the *Elcom* court inferred, then all software must be protected speech.[85]

This conclusion is problematic for two reasons. First, the court did not explain its focus on object code, rather than source code, when assessing defendant's circumvention software. Several courts declined to state definitively the status of object code,[86] which, if protected,

similarly *not* '*speech.*'" (emphasis added) (citing *Vartuli*, 228 F.3d at 111)). Note that in describing the *Vartuli* program as "not speech," *Corley* characterizes the *Vartuli* holding as addressing coverage, not protection. *Id.*

[81] *See Corley*, 273 F.3d at 449 ("*Vartuli* considered two ways in which a programmer might be said to communicate through code: to the user of the program (not necessarily protected) and to the computer (never protected).").

[82] The function of the circumvention technology, Advanced eBook Processer, is functionally similar to DeCSS, which acts upon DVDs. *See* United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1117–18 (N.D. Cal. 2002).

[83] *See id.* at 1126 (stating constitutional protection extends to both source code and object code). Recall object code is produced after a compiler interprets source code. *See supra* note 1.

[84] *Elcom*, 203 F. Supp. 2d at 1126 (citing Sony Comput. Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 602 (9th Cir. 2000)).

[85] *Id.* ("Computer software is expression that is protected by the copyright laws and is therefore 'speech' at some level, speech that is protected at some level by the First Amendment."). This statement ignores the fact that Congress may not define the limits of the First Amendment. *Cf.* City of Boerne v. Flores, 521 U.S. 507, 545 (1997) (O'Connor, J., dissenting) ("Congress lacks the ability independently to define or expand the scope of constitutional rights by statute."); New York v. United States, 505 U.S. 144, 156 (1992) ("Congress exercises its conferred powers subject to the limitations contained in the Constitution.").

[86] *E.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (confining constitutional analysis to source code); Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1139–43 (9th Cir.) (same), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999); Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2004) (assuming for purposes of action, without deciding, that executable code merits some constitutional protection); Junger v. Daley, 8 F. Supp. 2d 708, 715–17 (N.D. Ohio 1998) (confining constitutional

would ensure First Amendment coverage for all aspects of software.[87] Second, the court ignored that the case purporting to recognize the copyrightability of software did not state whether the program at issue contained any expressive content previous courts had found determinative of the First Amendment question.[88] Therefore, whether that software was an appropriate analogue to the DeCSS, for example, is unclear.

4. 321 Studios v. Metro Goldwyn Mayer Studios, Inc.

In the final decision to address the constitutional status of source code, the Northern District of California, two years after *Elcom*, rejected another constitutional challenge to the DMCA by plaintiffs who had engineered software similar to DeCSS.[89] Perhaps signaling a decisive shift in the judicial understanding of code as speech, the court recited: "Courts have held that computer code is speech, and therefore merits First Amendment protection."[90] The two cases the court cites and which remain good law, however—*Junger* and *Corley*—do not support such a categorical approach to software. To reiterate, *Junger* limited its constitutional analysis to the export of *source* code (not computer code generally).[91] And *Corley* arrives at its finding that "computer code, and computer programs constructed from code *can* merit First Amendment protection"[92] after acknowledging at least one type of code (code used to communicate with a computer) is "never protected" under its precedent.[93] The Northern District's misconstruction of its cited authorities therefore leads its analysis to proceed on the unsteady categorical premise that software generally merits First Amendment coverage.

---

analysis to source code), *rev'd*, 209 F.3d 481 (6th Cir. 2000); Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9–10 (D.D.C. 1996) (same).

87 Recall software requires source code, translated through a compiler, to create object code, which a computer may execute. See *supra* note 1 for a brief explanation of software.

88 Instead of describing the code's functional content, the court explained only its functional qualities. Sony Comput. Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 599–601 (9th Cir. 2008).

89 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1103–04 (N.D. Cal. 2004) (applying intermediate scrutiny).

90 Junger v. Daley, 209 F.3d 481, 484 (6th Cir. 2000); *321 Studios*, 307 F. Supp. 2d at 1099 (citing *Corley*, 273 F.3d at 445–49).

91 *See Junger*, 209 F.3d at 485 ("Because 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." (emphasis added)).

92 *Corley*, 273 F.3d at 449 (emphasis added). Compare *Corley*'s phrasing (specifically its use of the nonabsolute "can") with *321 Studios*'s more definite statement: "[C]omputer code *is* speech." *321 Studios*, 307 F. Supp. 2d at 1099 (emphasis added).

93 *Corley*, 273 F.3d at 449 (citing Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000)).

Ultimately, notwithstanding the holdings of *Corley*, *Elcom*, and *321 Studios*, the question remains unanswered: When used purely as a means to an end, does source code merit First Amendment coverage? *Corley* signals it should not, and *Elcom* and *321 Studios*'s uncritical recitations of precedent, itself subject to critique, offers scant substantive justification for its extension of constitutional scrutiny to computer code.

* * *

A review of the foregoing case law provokes four observations. First, some courts have declined even to answer the threshold question of whether the First Amendment applies to challenges of statutory restrictions on software. Of the seven cases discussed, two declined to take a definitive stance.[94] This hesitance to address the question may reflect, in part, the lack of a common First Amendment theory with which to approach the problem. Compare the district court's view in *Junger*, which said the First Amendment was adopted to foster the spread of ideas for bringing about political change,[95] with *Reimerdes*: "[Freedom of speech] discourages social violence by permitting people to seek redress of their grievances through meaningful non-violent expression."[96] Though neither contradicts the other, neither explains, without more, why source code should or should not be covered speech under the First Amendment. A stronger argument would consider an array of theories explaining the First Amendment's scope.[97]

Second, though five courts have offered constitutional coverage to source code, only three offered theories of free speech to explain its finding,[98] and none is entirely comprehensive. Both *Junger* and *Corley*

---

[94] *See* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 219–20 (S.D.N.Y. 2000) (assuming, without deciding, executable code merits protection); Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) (assuming the purpose of deciding the case's dispositive issue source code merits protection). Additionally, the district court in *Junger* discussed the constitutional status of source code without deciding the question of its protection, Junger v. Daley, 8 F. Supp. 2d 708, 715–18 (N.D. Ohio 1998).

[95] *Junger*, 8 F. Supp. 2d at 715–16 (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).

[96] *Reimerdes*, 82 F. Supp. 2d at 221–22 (citing Whitney v. California, 274 U.S. 357, 375 (Brandeis, J. & Holmes, J., concurring) (1927), *overruled by* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969)).

[97] See *infra* Section II.A for a fuller discussion on how theoretical justifications for free speech doctrine may explain the constitutional status of encryption source code.

[98] *Elcom* bases its assertion of source code's constitutional status by citing case law finding source code copyrightable (assuming without explanation that all copyrightable material is also protected speech). 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002). *321 Studios* grounds its argument with citations to case law, 307 F. Supp. 2d 1085, 1099 (N.D. Cal. 2004), which provide uncertain support for the proposition. *See supra* notes 91–93

(and the withdrawn *Bernstein* opinion) emphasized the expressive quality of code.[99] But whereas *Junger* would apply its holding to all source code (because source code is capable of human comprehension),[100] *Corley* carved out code that communicates with a computer as beyond the Constitution's ambit.[101] *Corley* indicated while expressiveness of source code matters, the identity of the receiver of that expression may decide the constitutional status of the source code.[102] Therefore, even the courts which have stated an opinion on the status of source code do not agree on what it means for supposed speech to be expressive for First Amendment purposes, again suggesting a lack of a common normative theory with which to approach coded language.

Third, the foregoing cases, despite their inconsistent approaches to the question of the constitutional status of source code, largely recognize there is a legally significant difference between code performing a communicative function and code performing a mechanical one: *Karn* distinguishes source code without comments (functional) from code with comments (expressive);[103] *Bernstein* limited its analysis to code as used in cryptography, a distinctly expressive activity;[104] *Junger* held source code protected speech because it is expressive, not functional;[105] *Reimerdes* described source code as a "virtual machine" rather than an expressive instrument;[106] and *Corley* acknowledged

(explaining the court's reasoning). The Ninth Circuit found source code, as it is used by those in the cryptography field, to be covered speech; it withdrew its opinion, however. Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

99 *Compare* Junger v. Daley, 209 F.3d 481, 484 (6th Cir. 2000) ("The fact that a medium of expression has a functional capacity should not preclude constitutional protection."), *with* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 446–47 (2d Cir. 2001) (quoting Bd. of Trustees of Leland Stanford Junior Univ. v. Sullivan, 773 F. Supp. 472, 474 (D.D.C. 1991)) (characterizing source code as scientific expression covered by the Constitution). *See also* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1142 (9th Cir.) ("The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution."), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

100 *See Junger*, 209 F.3d at 484 (stating cryptographers generally use source code to communicate).

101 *Corley*, 273 F.3d at 449 (stating that communications to a computer are "never protected" (citing Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94 (2d Cir. 2000))).

102 *See id.*

103 *See* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) ("The Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment. Source codes are merely a means of commanding a computer to perform a function.").

104 *See supra* notes 58–62 and accompanying text.

105 *See supra* note 54 and accompanying text.

106 *See supra* note 74 and accompanying text.

source code communicating with a computer as distinct from code communicating to people.[107] *Elcom* and *321 Studios*, whose sweeping holdings are tenuous,[108] are outliers by comparison.

Fourth, and most important: No court has considered the constitutional status of source code not subject to, or incapable of, third-party review. The cases above agree programmers use source code as a means of communication with each other, and therefore source code contains some expressive quality; because of this expressiveness, source code merits First Amendment coverage.[109] But what if a programmer creates source code purely as a means to an end, with neither the intention nor expectation of peer review—what I term purely functional source code?[110] Such a scenario is not hypothetical. If forced to comply with a court order demanding the creation software to circumvent encryption technology on a device subject to a law enforcement investigation, the manufacturer would keep that software secret to avoid its use by private actors.[111] When law enforcement next seeks such an order, the reviewing court will confront this issue: Is that code covered, and if so why?[112]

II
How Courts Should Assess the Constitutional Status of Source Code

In Part I, I described how courts have assessed the constitutional status of source code, arguing that the case law fails to answer the question of whether purely functional source code is speech. Now, in Part II, I suggest how courts should address this question.

---

107 *See supra* notes 79–80 and accompanying text (discussing *Corley*'s acknowledgement of *Vartuli*).

108 *See supra* Section I.B.3–4 (critiquing the analyses in these cases).

109 *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 446 (2d Cir. 2001) (relating the expressiveness of source code with communication among programmers, and code's First Amendment protection); Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir. 1999) (same). *Reimerdes*, *Karn*, and the *Junger* district court do not speak definitively on the constitutional status of source code. *See supra* note 94.

110 *See supra* notes 25–28 and accompanying text (distinguishing purely functional source code from expressive source code).

111 *See* Cook, *supra* note 19 ("Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.").

112 In his commentary on *Bernstein* one scholar declined to answer this precise question, saying this scenario presents a "messier" question, with an answer "more difficult to formulate and enforce," than those raised under the federal regulations responsible for the above cases. Robert Post, *Encryption Source Code and the First Amendment*, 15 Berkeley Tech. L.J. 713, 720 (2000).

But first, a preface: The Court has never announced a definitive standard to distinguish covered speech from noncovered speech.[113] When presented with a close question, courts are inclined to assume the presence of speech than to decide the question definitively.[114] In explaining this reluctance, one scholar wrote, "The First Amendment's coverage questions are difficult because the normal tools for delineating the coverage of a constitutional rule are unavailing."[115] The Fourth Amendment's operative term "seizure" and the Eighth's "punishment," for example, provide more inherent interpretative guidance than the First Amendment's "speech," which does not have as intuitive a meaning.[116] There being no definitive test to distinguish covered speech from noncovered speech,[117] I here embark on an analysis borrowing from the approach taken by above-mentioned case law and First Amendment scholarship.[118]

---

113 In *Spence v. Washington*, the Court provided a test to identify expressive conduct meriting First Amendment protection, but not for all speech. 418 U.S. 405, 410–11 (1974) (per curiam) (holding "[a]n intent to convey a particularized message" that "in the surrounding circumstances the likelihood [would be] great that the message would be understood by those who viewed it" is required to find expressive conduct covered by the First Amendment).

114 *See* R. George Wright, *What Counts as "Speech" in the First Place?: Determining the Scope of the Free Speech Clause*, 37 PEPP. L. REV. 1217, 1227 (2010) ("[A] number of courts, when faced with borderline speech, have merely assumed the putative speaker to have engaged in speech . . . . [F]or the sake of the argument, speech is assumed, and the court must then find some legitimate way to conclude . . . the regulation can nonetheless be upheld."); *see also id.* at 1227 n.56 (collecting cases). Courts have done the same in the context of software. *See* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9 (D.D.C. 1996) (assuming without deciding the presence of speech in a challenge to an export restriction on encryption software).

115 Schauer, *supra* note 29, at 1772–73.

116 In distinguishing the First Amendment's use of the amorphous term "speech" with other, more precise, words used elsewhere in the Constitution, Schauer notes, "We may often debate about which seizures are unreasonable and about which punishments are cruel and unusual, but disagreements about whether we are dealing with a seizure or a punishment are comparatively rare." *Id.* at 1772.

117 By way of reinforcing the notion that covered speech is not easily distinguished from noncovered speech, see generally Schauer, *supra* note 29 (surveying the boundaries of First Amendment coverage but without offering an explanatory theory); Daniel F. Wachtell, Note, *No Harm, No Foul: Reconceptualizing Free Speech Via Tort Law*, 83 N.Y.U. L. REV. 949, 950 (2008) (observing "no logical lines can reasonably be drawn to separate speech from nonspeech" and offering an original approach to defining speech); Wright, *supra* note 114 (noting the difficulty of defining speech and surveying an array of analytical approaches).

118 In doing so, I accept in part one scholar's invitation to "consult history, original intentions, *moral theory*, *tradition*, or any of the other conventional, albeit contested, sources of constitutional guidance . . . ." Schauer, *supra* note 29, at 1773 (emphasis added). *See infra* notes 122–23 and accompanying text (noting previous courts' reference to normative theories discussed in Section II.A).

Accordingly, I divide this Part in two Sections, each exploring an independent mode of distinguishing covered speech from nonspeech: First, Section A elaborates and improves upon an approach courts have used and may adopt when confronted with the question of the constitutional status of source code. This approach defines speech as communication whose substance serves a normative interest underlying the First Amendment. Second, Section B engages an approach defining speech as communication regulated with improper governmental purpose.[119] I conclude neither mode justifies First Amendment coverage for purely functional source code.

A. Determining the Scope of Speech by Substance

The argument that the substance of a communication indicates its constitutional status assumes that only communications advancing some interest underlying the principle of free speech may qualify as speech within the meaning of the Constitution.[120] Accordingly, in the following pages, I outline four rationales frequently identified by courts and scholars as justifying the free speech principle and assess how each may be used to justify (or deny) constitutional coverage of purely functional source code. In particular, I address, in order, the marketplace-of-ideas rationale, the democratic self-governance rationale, and the individual autonomy rationale.[121] I then turn to a novel

---

[119] I explain in greater detail this approach *infra* Section II.B. For now, I underscore the following: Government motive figures prominently when assessing regulations under various levels of First Amendment scrutiny. *See* 1 SMOLLA & NIMMER, *supra* note 49, §§ 3.3–.4 (discussing the importance of governmental motive in assessing regulations of covered speech). But whereas such tests presume the existence of speech, this mode of analysis says that in determining whether First Amendment scrutiny applies at all, speech itself can be "discovered" by reference to government motives. *See* Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1255–56 (1995) ("There are . . . two independent kinds of considerations that have in fact triggered First Amendment scrutiny. The first involves the question of what is being regulated . . . . The second involves the question of why the state seeks to regulate . . . ."). For a similar discussion emphasizing the significance of governmental motive for regulations of communication, see Elena Kagan, *Private Speech, Public Purpose: The Role of Governmental Motive in First Amendment Doctrine*, 63 U. CHI. L. REV. 413, 516 (1996), arguing "most of First Amendment doctrine constitutes a highly, but necessarily, complex scheme for ascertaining the governmental purposes underlying regulations of speech."

[120] *See* Post, *supra* note 119, at 1255 ("First Amendment analysis is relevant only when the values served by the First Amendment are implicated.").

[121] I exclude for the sake of space—but recognize the importance of also considering—certain theories courts have not widely embraced in interpreting the First Amendment. These theories include the "dissent theory," according to which free speech doctrine is designed to sponsor "the spirit of nonconformity within us all," *see* STEVEN H. SHIFFRIN, THE FIRST AMENDMENT, DEMOCRACY, AND ROMANCE 5 (1990); "tolerance theory," according to which free speech serves to expose individuals to a diversity of ideas, *see* LEE C. BOLLINGER, THE TOLERANT SOCIETY 6–11 (1986); and various eclectic theories, *see*

theory defining the scope of the First Amendment according to the social context in which the putative speech occurs.

I adopt this approach because it aligns with courts' method of distinguishing speech from nonspeech. In the encryption source code context, courts gestured toward principles traditionally understood to justify the First Amendment. For example, *Bernstein* said code formed an aspect of the search for truth;[122] *Remeirdes* suggested code may serve the interest of democratic self-governance.[123] But no court has analyzed source code under a broad array of normative theories. By explaining and testing the application of these normative rationales with reference to purely functional source code, I demonstrate no rationale, alone or in combination with others, requires recognizing such code as covered speech.

1. The Marketplace-of-Ideas Rationale

The first, and perhaps the most familiar, of the interests underlying the First Amendment is the maintenance of a marketplace of ideas. In the Court's words, "[i]t is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail . . . ."[124] But not all ideas contribute to the discovery of truth. For example, Justice Holmes wrote, "the First Amendment . . . cannot have been, and obviously was not, intended to give immunity for every possible use of language."[125]

MATTHEW D. BUNKER, CRITIQUING FREE SPEECH: FIRST AMENDMENT THEORY AND THE CHALLENGE OF THE INTERDISCIPLINARITY 17 (2001) (describing hybrid theories of the First Amendment). I focus my analysis on the first three because of their prominence in First Amendment commentary, and on the fourth because it has been used specifically in describing the constitutional status of encryption source code.

122 *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.) (describing source code's use as a language of scientific research), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

123 *See* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 221 (S.D.N.Y. 2000) (noting First Amendment justifications, though recognizing certain theories, do not support encryption source code's classification as speech).

124 Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (holding that the fairness doctrine advanced the interests of the First Amendment by insuring a balanced discussion of issues). *See also* Columbia Broad. Sys., Inc. v. Democratic Nat'l Comm., 412 U.S. 94, 184 (1973) (Brennan, J., concurring) ("[I]n light of the unique nature of the electronic media, the public have strong First Amendment interests in the reception of a full spectrum of views . . . ."); Adler v. Bd. of Educ., 342 U.S. 485, 511 (1952) (Douglas, J., dissenting) ("[I]t was the pursuit of truth which the First Amendment was designed to protect."); Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market . . . .").

125 Frohwerk v. United States, 249 U.S. 204, 206 (1919) (citing Robertson v. Baldwin, 165 U.S. 275, 281 (1897) (stating, in refusing to recognize conspiratorial conduct as covered speech, "[w]e venture to believe that neither Hamilton nor Madison, . . . ever supposed

Accordingly, in finding source code constitutionally covered speech, courts often have described code as necessary to scientific expression. *Bernstein* observed cryptographers use encryption source code "to facilitate the precise and rigorous expression of complex scientific ideas."[126] The court also suggested plaintiff's publication of his source code constituted a political expression, an attempt to challenge the statutory regulations on encryption technology export.[127] Courts generally have not considered, however, the status of code not intended to advance the science of cryptography, to instruct novice coders, or to challenge public policy.[128] For if they did, they would need another basis on which to justify the protection granted to encryption source code.

The marketplace theory presupposes a community of more than one. This is inherent in the words "exchange,"[129] "discussion,"[130] and "debate"[131] often used to describe the principle. Just as a thought unsaid does not advance a conversation, private speech—speech not shared—has no value to the ideas marketplace insofar as it does not contribute directly to the discovery of truth. Likewise, a line of code written by a programmer who then uses it in a private project—as when compelled by court order, say—does not thereby further computer science, instruct novice code writers, or challenge public policy. Courts offer no response to this critique, though in fairness, they have not had reason to. Existing case law treats source code intended for sharing, whether for the academy or the market.[132] And the one case

---

that to make criminal the counselling of a murder within the jurisdiction of Congress would be an unconstitutional interference with free speech.")).

126 *Bernstein*, 176 F.3d at 1141. *See also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 448 (2d Cir. 2001) (describing the educational value of studying source code).

127 *Bernstein*, 176 F.3d at 1141 n.14.

128 The notable exception is *Corley*, 273 F.3d at 449 (stating communications by a programmer to a computer through code are "never protected").

129 *See, e.g.*, *Columbia Broad. Sys., Inc.*, 412 U.S. at 187 (Brennan, J., dissenting) (restating the constitutional objective "to provide the kind of uninhibited, robust, and wide-open exchange of views" (internal quotations omitted)).

130 *See, e.g.*, Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) (describing the clear-and-present danger test and stating "[i]f there be time to expose through *discussion* the falsehood and fallacies . . . the remedy to be applied is more speech" (emphasis added)), *overruled by* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969).

131 *See, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279 n.19 (1964) ("Even a false statement may be deemed to make a valuable contribution to public *debate* . . . ." (emphasis added)).

132 *See supra* Sections I.A–B (discussing export restriction cases that involved exports purporting to share their technology with others in their field and DMCA cases that involved programmers distributing decryption software for readers and film audiences).

that did acknowledge this potential for private speech, *Corley*, accepted such code never merits constitutional coverage.[133]

Critics of this analysis may argue that while not all source code is subject to review by individuals other than the author, the fact that it *may* be reviewed renders all source code an aspect of scientific discussion.[134] But certain speech acts, despite belonging to the same "genre," are not similarly protected.[135] That the First Amendment covers advertisements,[136] for example, does not mean it covers all advertisements;[137] that the First Amendment covers truthful commercial communications[138] does not mean it covers all truthful communications made pursuant to a commercial transaction.[139] Viewed this way, sweeping statements like "computer code is speech, and is therefore protected by the First Amendment"[140] and "encryption software, in its source code form and as employed by those in the field of cryptography . . . [is] expressive for First Amendment purposes"[141] go too

---

133 Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001) (citing Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000)).

134 *Bernstein*, for example, suggests that while source code "is destined for the maw" of a computer, the fact that "it can be used to express an idea or method" weighs decisively in favor of finding encryption source code protected speech. *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1140 (9th Cir.), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

135 *See, e.g.*, Schauer, *supra* note 29, at 1766–67 & nn.1–6 (discussing speech categories that may be excluded from First Amendment coverage).

136 *See, e.g.*, Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976) (finding commercial speech protected under the First Amendment).

137 Securities-related commercial speech does not invoke First Amendment scrutiny, for example. Courts have denied arguments that the First Amendment restricts the Securities and Exchange Commission's enforcement of statutory antifraud measures. *See, e.g.*, U.S. Sec. & Exch. Comm'n v. Pirate Inv'r LLC, 580 F.3d 233, 255 (4th Cir. 2009) (stating, in its rejection of a First Amendment challenge to the antifraud provision of the Securities Exchange Act, "[p]unishing fraud, whether it be common law fraud or securities fraud, simply does not violate the First Amendment"); *see also* Wendy Gerwick Couture, *The Collision Between the First Amendment and Securities Fraud*, 65 ALA. L. REV. 903, 905 (2014) (noting the failure of First Amendment challenges to securities advertisements); Lloyd L. Drury, III, *Disclosure Is Speech: Imposing Meaningful First Amendment Constraints on SEC Regulatory Authority*, 58 S.C. L. REV. 757, 761 (2007) (recognizing securities disclosures are not considered commercial speech despite commercial characteristics); Schauer, *supra* note 29, at 1778–79 (recognizing no First Amendment scrutiny applies to determine the constitutionality of content-based advertising restrictions of the Securities Act).

138 *See* Bates v. State Bar of Ariz., 433 U.S. 350, 381–82 (1977) (finding attorneys' publication of fee information protected by the First Amendment).

139 *See* Schauer, *supra* note 29, at 1781 ("[A]ntitrust law restricts the exchange of accurate market, pricing, and production information, as well as limits the advocacy of concerted action in most contexts; yet it remains almost wholly untouched by the First Amendment." (internal citations omitted)).

140 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1093 (N.D. Cal. 2004).

141 Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

far. If the marketplace theory of the First Amendment prevails,[142] courts must treat source code as it would any other language—divisible by genre—and exclude from coverage those forms not adding to the exchange of ideas. Accordingly, courts would exclude from coverage purely functional source code,[143] including that designed to circumvent encryption architectures.

2. The Democratic Self-Government Rationale

The second grounding theory, closely related to the first, would protect communication necessary to inform democratic decision-making.[144] A leading proponent of the democratic self-governance rationale explained, "[s]elf-government can exist only insofar as the voters acquire the intelligence, integrity, sensitivity, and generous devotion to the general welfare that . . . casting a ballot is assumed to express."[145] To acquire these attributes, the government must protect not only political speech,[146] but also other forms of expression "from

---

[142] That courts will continue to abide to this theory is not beyond doubt. *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 592 (1980) (Rehnquist, J., dissenting) ("There is no reason for believing that the marketplace of ideas is free from market imperfections any more than there is to believe that the invisible hand will always lead to optimum economic decisions in the commercial market."); C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964 (1978) (critiquing the classic model of the marketplace theory).

[143] Recall my definition of terms, *supra* notes 25–27, characterizing purely functional source code as code not designed to participate in scientific, educational, or other interpersonal dialogue. This subgenre of code lacks justification under this rationale for coverage under the First Amendment. By contrast, other forms of code, what I term "expressive source code," necessarily participate in such dialogue and therefore may merit coverage.

[144] *See* ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 75 (1960) (arguing the "primary purpose of the First Amendment is . . . that all the citizens shall, so far as possible, understand the issues which bear upon our common life"); ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 26 (1948) ("[I]t is th[e] mutilation of the thinking process of the community against which the First Amendment to the Constitution is directed."); *see also* Cass R. Sunstein, *Free Speech Now*, 59 U. CHI. L. REV. 255, 305 (1992) ("There can be little doubt that suppression by the government of political ideas that it disapproved, or found threatening, was the central motivation for the clause. The worst examples of unacceptable censorship involve efforts by government to insulate itself from criticism."). The Court has often noted the connection between self-government and First Amendment rights. *E.g.*, McCutcheon v. Fed. Election Comm'n, 134 S. Ct. 1434, 1448 (2014) ("The First Amendment 'is designed and intended to remove governmental restraints from the arena of public discussion . . . in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests.'" (quoting Cohen v. California, 403 U.S. 15, 24 (1971))).

[145] Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 255–57.

[146] For a discussion on the importance of political speech to the principle of self-government, see Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339 (2010) ("The

which the voter derives . . . knowledge, intelligence, [and] sensitivity to human values," including education, the arts, and the sciences.[147] Understanding the First Amendment this way may help further clarify courts' refusal to entitle some forms of communication full constitutional protection. For example, copyright, securities, and antitrust violations serve no apparent political purpose and are duly excluded from First Amendment coverage.[148]

Now, consider source code's value as a means of democratic decision-making. In circumstances where a programmer communicates code to a colleague, he may be engaged in the scientific exchange of ideas[149] or education.[150] If this pedagogical communication thereafter enhances the public dialogue on which this theory of the First Amendment is premised,[151] then perhaps this source code merits constitutional coverage.[152] But if a programmer does not communicate their source code to another, their code falls outside the scope of speech under the democratic self-governance theory. The reason is substantially similar to the analysis presented under the marketplace-of-ideas rationale.[153] Like the marketplace principle, the self-government theory defines speech relative to its capacity to advance a

---

right of citizens to inquire, to hear, to speak, and to use information to reach consensus is a precondition to enlightened self-government and a necessary means to protect it. The First Amendment has its fullest and most urgent application to speech uttered during a campaign for political office." (internal quotation marks and citations omitted)); *id.* at 452, 473–74, 478–79 (Stevens, J., dissenting) (citing self-government to argue against the principle that corporate campaign expenditures merit First Amendment protection).

147 Meiklejohn, *supra* note 145, at 256. In recognizing these knowledge-creating forms of communication, Meiklejohn averts the criticism that the theory is underinclusive, protective of public political speech and nothing else. *See generally* Zechariah Chafee, Jr., *Free Speech: And Its Relation to Self-Government*, 62 HARV. L. REV. 891, 900 (1949) (reviewing ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948)) (arguing that if Meiklejohn's definition of speech excludes "art and literature, it [would be] shocking to deprive these vital matters of the protection of . . . the First Amendment").

148 *See* Schauer, *supra* note 29, at 1771 ("In these and countless other instances, the permissibility of regulation—unlike the control of incitement, libel, and commercial advertising—is not measured against First Amendment-generated standards."); *see also id.* at 1766–67 nn.1, 2 & 5 (collecting cases).

149 *See, e.g.*, Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.) (noting how cryptographers use source code "to facilitate the precise and rigorous expression of complex scientific ideas"), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

150 *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 448 (2d Cir. 2001) (describing how programmers use source code to improve their skills).

151 For example, perhaps the study of cryptography informs the electorate of the potential scope of government surveillance.

152 *See supra* note 147 and accompanying text (noting self-governance theory accepts knowledge-producing modes of communication as protected speech).

153 *See supra* notes 129–31 and accompanying text (arguing the marketplace theory assumes a community of more than one).

dialogue, in this case a broad, nationwide political debate. This conversation aims not to uncover truths, but to discover and advance political outcomes chosen by a fully informed electorate. By abstaining from public conversation, the programmer communicating alone or to a computer does not further this goal, and therefore does not merit coverage under this principle.

3. The Individual Autonomy Rationale

A third, broader, grounding theory of the First Amendment recognizes that free expression has inherent value. According to Justice Brandeis, "[t]hose who won our independence believed that the final end of the state was to make men free to develop their faculties . . . . They valued liberty both as an *end* and as a means."[154] This argument has it that our "dignity as individual people and as a culture depends upon our being able to claim meaning for our lives and experience" through speech that develops the mind first and society second.[155]

While compelling in theory, the rationale in fact does little to delimit the term "speech" as used in the Constitution. For example, this theory would require the First Amendment to protect the tinkering of the craftsman because their hobby constitutes an aspect of their personality. In practice, of course, courts would not, because neither the act of creation nor the object created rises to the level of expressive conduct.[156] Likewise, this theory justifies protecting the artist who creates a painting because art "figures predominantly into our vague notion of what it means to be human."[157] Indeed, in practice courts *do* protect the artist, but not because the act of creation is "uniquely human"[158] or even because the act is expressive, but because art itself is speech.[159]

---

154 Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring) (emphasis added), *overruled by* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969).

155 *See* James Boyd White, *Free Speech and Valuable Speech: Silence, Dante, and the "Marketplace of Ideas,"* 51 UCLA L. REV. 799, 818 (2004) (distinguishing this theory from the marketplace-of-ideas theory). For a more comprehensive discussion on the individual autonomy theory of the First Amendment, see generally Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RES. J. 521, 544–48; Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 623–29 (1982).

156 Imagine, for example, a hobbyist building a playground for his children, where an "intent to convey a particularized message" does not exist. Such activity would not be speech under the First Amendment doctrine. *See* Spence v. Washington, 418 U.S. 405, 410–11 (1974) (per curiam) (explaining the standard for expressive conduct protected under the First Amendment). I discuss Spence in greater depth *infra* Section II.A.4.

157 Blasi, *supra* note 155, at 544 (describing "individual autonomy" theory).

158 Redish, *supra* note 155, at 628.

159 *See* Hurley v. Irish-Am. Gay, Lesbian and Bisexual Grp. of Boston, 515 U.S. 557, 569 (1995) (finding that painting, music, and poetry are "unquestionably shielded" by the First Amendment); Sonya G. Bonneau, *Ex Post Modernism: How the First Amendment Framed*

Applying individual autonomy theory to the programming context, we may appreciate the project of code writing is, like the craftsman's or the artist's labor, inherently rewarding. But a court should not, for that reason, extend First Amendment coverage to the programmer's conduct. Source code not intended for review and serving a purely utilitarian purpose does not constitute expression like the artist's painting;[160] it is more like the craftsman's project.[161] As *Reimerdes* stated, source code "is best treated as a virtual machine,"[162] a means to an end rather than an end in itself. If, on the basis of an individual autonomy theory, a machine entitles First Amendment protection to its creator, all material objects would invoke the same treatment, thereby expanding the scope of the First Amendment and emptying it of content.[163]

Nonrepresentational Art, 39 COLUM. J.L. & ARTS 195, 221 (2015) ("Recent Supreme Court decisions are not merely welcoming of visual media, but have situated it on the highest rung of speech protection, triggering strict scrutiny of any form of government regulation."). I am aware of no case finding the act of creation of a work of art—except performance art—is constitutionally protected speech, though I recognize under *Spence* such an act may qualify if done with the intent to convey a particularized message. *See, e.g.*, Berger v. City of Seattle, 569 F.3d 1029, 1035–36 (9th Cir. 2009) (en banc) (applying First Amendment scrutiny to street performances).

160 *See infra* Section II.A.1 (describing the lack of expressiveness of a certain genre of encryption source code).

161 The dissenting opinion in *Bernstein* makes this argument: "Encryption source code is a building tool. . . . [T]he ultimate purpose of encryption source code is, as its name suggests, to perform the function of encrypting messages." Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1148 (9th Cir.) (Nelson, J., dissenting), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

162 Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 222 (S.D.N.Y. 2000) (citing Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 236 (1998) ("We think most executable software is best treated as a virtual machine rather than as protected expression." (italics omitted))). *But see Bernstein*, 176 F.3d at 1142 (rejecting "the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution"); Steven E. Halpern, *Harmonizing the Convergence of Medium, Expression, and Functionality: A Study of the Speech Interest in Computer Software*, 14 HARV. J.L. & TECH. 139, 142–45 (2000) (describing the obvious functionality of object code relative to the more expressive source code from which it is derived).

163 *See* Kent Greenawalt, *Free Speech Justifications*, 89 COLUM. L. REV. 119, 145 (1989) ("An argument based on the value of liberty as [a] . . . means of personal development is not restricted to speech alone. Indeed, it may reach widely and strongly enough to some other matters so that alone it would not warrant anything properly identified as a distinctive principle of free speech."). Others have not adopted as absolutist an approach. For example, one author wrote, in a critique of this theory, "the value of self-realization [is] furthered by unintrusive regulations designed to protect individuals living and operating within a political unit." Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015, 1033–34.

4. The Social Context Rationale

A discussion of the First Amendment's substantive scope might have begun with *Spence v. Washington*.[164] There, the Court held First Amendment scrutiny applies to conduct when "[a]n intent to convey a particularized message [is] present, and in the surrounding circumstances the likelihood [is] great that the message would be understood by those who view[ ] it."[165] The particularized message need not be "narrow [and] succinctly articulable."[166]

But scholars have called this test incomplete,[167] as it would protect antisocial activities like the act of driving over the speed limit in protest of the government, for example.[168] In response, Robert Post argues, courts must consider, as a limiting principle, the social context in which communicative acts are performed.[169] Accordingly, "[t]he unit of First Amendment analysis . . . ought not to be speech, but rather particular forms of social structure."[170] In other words, look not to speech, but to whom it is said and where. Therefore, some social contexts may "render individual acts of communication [like speeding] into events without First Amendment protection."[171]

From this perspective, myriad restrictions on speech not invoking First Amendment coverage become more easily understood, for instance: contempt statutes enforcing compelled testimony of immu-

---

164 *See, e.g.*, Susan H. Williams, *Content Discrimination and the First Amendment*, 139 U. PA. L. REV. 615, 646 n.132 (1991) (describing *Spence* as the first case to address the definition of expressive conduct head-on). Though *Spence* may be the most lucid test to identify First Amendment speech, it is not directly applicable here. *Spence* provides a means to identify expressive conduct protected under the First Amendment. It does not control the question of the constitutional status of a form of language.

165 Spence v. Washington, 418 U.S. 405, 410–11 (1974) (per curiam) (holding unconstitutional a state flag-desecration statute as applied to a student). *See also* Texas v. Johnson, 491 U.S. 397, 403 (1989) (applying the *Spence* test to a flag desecration).

166 Hurley v. Irish-Am. Gay, Lesbian and Bisexual Grp. of Boston, 515 U.S. 557, 569 (1995) (holding unconstitutional a state statute requiring inclusion in a parade of members whose message contradicts the organizers').

167 *See, e.g.*, Post, *supra* note 119, at 1252 ("[T]he [*Spence*] doctrine is transparently and manifestly false. The test cannot plausibly be said to express a sufficient condition for bringing the First Amendment into play." (internal quotation marks omitted)); Jed Rubenfeld, *The First Amendment's Purpose*, 53 STAN. L. REV. 767, 773 (2001) ("*Spence* is a profoundly unsatisfactory test for deciding what nonverbal stuff counts as sufficiently 'expressive' to trigger First Amendment scrutiny.").

168 *See* Rubenfeld, *supra* note 167, at 772–74 (describing how *Spence* would approach this problem).

169 *See* Post, *supra* note 119, at 1254 (suggesting that First Amendment analysis is only relevant when the values served by the Amendment are implicated, and that these values are implicated by the social context in which speech acts are performed, not the speech acts themselves).

170 *Id.* at 1273.

171 *Id.* at 1255.

nized witnesses, hostile-environment laws prohibiting harassment in the workplace, securities regulation restricting corporate communications to the market, and rules of professional responsibility barring disclosure of confidential information.[172] In each example, where First Amendment objections do not apply, regulations on communication support the social structure in which the speaker acts.

It follows that under this social context theory a court would inquire into the circumstances of the sale and application of encryption code.[173] For example, encryption source code written to form an aspect of academic dialogue would merit constitutional coverage because it advances the science of cryptography. Source code not written to participate in a dialogue would not merit constitutional coverage because it offers no such benefit to society. Post responds by noting, "even if encryption source code is not itself a subject of public discussion, its regulation might nevertheless affect public discussion in ways that ought to trigger First Amendment coverage."[174]

Normatively, this sounds compelling. Government regulation of encryption may chill the conduct of creators of purely functional source code. However, creators of such code do not generally engage in this conduct,[175] except when circumstances require secrecy—such as industry practice or a court order. And if the circumstances require writing purely functional source code, government regulations may not be expected to decrease its production.[176] Alternatively, regulations could depress the market for technologies using encryption, just as news of government surveillance grew it.[177] More dramatically, regulations of encryption may chill public debate occurring by way of encryption.[178] For example, in *City of Lakewood v. Plain Dealer Publishing, Co.*, the Court said when a government licensing regulation

---

172 *See* Schauer, *supra* note 29, at 1765–67 (exploring when and why the First Amendment is implicated).

173 *See* Post, *supra* note 112, at 720 (applying this theory to encryption source code).

174 *Id.* at 721.

175 Most source code, as courts have intimated, is intended for communicative purposes. *See, e.g.*, Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1141 (9th Cir.) (noting the communicative utility of source code), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

176 Stated differently: One cannot argue source code created *because* a court order requires its creation will be less likely to be written because of the threat of a court order.

177 *Cf.* DANIEL CASTRO & ALAN MCQUINN, UNLOCKING ENCRYPTION: INFORMATION SECURITY AND THE RULE OF LAW 14–21 (2016), http://www2.itif.org/2016-unlocking-encryption.pdf (describing how compromising encryption decreases users' security); LEWIS ET AL., *supra* note 3, at 2 (describing how the market for encrypted devices grew in response to security concerns).

178 *See* Geoffrey Gordon, Note, *Breaking the Code: What Encryption Means for the First Amendment and Human Rights*, 32 COLUM. HUM. RTS. L. REV. 477, 504 (2001) (noting the importance of encryption to human rights activists working in oppressive regimes); *supra* notes 4–5 (noting the significance of encrypted technologies' everyday applications).

specifically targets conduct commonly associated with expression, such a licensing scheme may constitute an unlawful prior restraint on speech.[179] In particular, the Court expressed concern that targeting speech-producing conduct would engender self-censorship.[180] Similar arguments have been proposed by those who say encryption source code merits constitutional protection.[181]

To assess whether these secondary effects on public discussion ought to trigger First Amendment coverage, Post says courts must consider, first, the effects of government regulation of encryption source code both on the production or use of encryption software and, second, on the various media that employ encryption software.[182] Decreased production or use of software and its applications may indicate the type of self-censorship *Lakewood* forbids.

Imagine, then, two hypotheticals involving purely functional source code. First, consider the dramatic scenario in which a government-mandated "backdoor" compromises the encryption architecture on all mobile devices on the market.[183] If no device offers complete security, consumers' preferences may not change at all. Perhaps a subset of consumers would decline to participate in a market not offering perfect security. But without data, estimates of that market effect remain speculative. More likely, consumers would refrain from communicating sensitive data using their devices (though, again, the effect remains hypothetical). Under a theory defining constitutional speech relative to social structures in which the speaker acts, these potentially substantial social costs would suggest encryption source code would function as speech for First Amendment purposes.[184]

Now consider the real scenario, the one where the government required a manufacturer to write a program enabling access to a crim-

---

179 486 U.S. 750, 759–62 (1988) (holding unconstitutional an ordinance granting a mayor authority to deny applications for permits to place news racks on public property).

180 *Id.* at 759 (allowing a facial challenge to a state licensing statute due, in part, to a risk that speakers would self-censor to avoid being denied a license to speak).

181 *See* Gordon, *supra* note 178, at 513–15 (citing *Lakewood* to argue the EAR violates prior restraint doctrine); Post, *supra* note 112, at 723 ("Encryption software is a way of preventing an analogous chill within digital media.").

182 Post, *supra* note 112, at 722. Post declines to answer the question of whether these secondary effects trigger First Amendment scrutiny. He offers this framework with which to analyze the problem.

183 *See Perils of Back Door Encryption Mandates*, HUMAN RIGHTS WATCH (June 26, 2017, 10:52 AM), https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates (describing the "back door" approach to government access to encrypted data).

184 Post would ask, also, about the effects on various First Amendment media that use encryption software and whether this impact would raise sufficient constitutional concerns as to merit First Amendment coverage. *See* Post, *supra* note 112, at 722.

inal suspect's encrypted device.[185] In a similar situation, the circumstance's specificity—the singular phone, the singular program—mitigates the market impact relative to the first scenario in which the government disables all devices' encryption software.[186] The effects on speech would also be lessened, if they exist at all. Admittedly, no polling data indicates shifts in consumer preferences resulting from law enforcement access to encryption on mobile devices. However, I suggest the chilling effect on speech would be minimal based on an analogy to nondigital forms of data protection. In the same way encryption makes information inaccessible to anyone without the key—generally a series of numbers—safes protect information from those without the combination.[187] Despite the threat of a third party compromising its security features, safes and other mechanical forms of file protection are widely used for lack of an alternative.[188] By analogy, the threat of "cracking" a single device may not diminish necessarily the attractiveness of digital data protection technologies, for there is currently no apparent alternative. Other legal protections exist to ensure the use of these measures respects individual privacy interests.[189] And though the manufacturer would always, in theory, develop the required circumvention software, they would act as agents of law enforcement, never on their own volition.

Therefore, under the same social context theory, but in light of a different form of regulation, First Amendment coverage would not apply at all to encryption source code.

---

[185] The FBI aimed to use this surgical approach to accessing encrypted data during its dispute with Apple. *See supra* notes 12–15 and accompanying text (describing the FBI's efforts to circumvent a device's encryption pursuant to a criminal investigation).

[186] Privacy advocates liken specialized software created to access one device to a universal backdoor. Such software, they argue, may be used "again and again, for other phones." Kurt Opsahl, *EFF to Support Apple in Encryption Battle*, ELEC. FRONTIER FOUND. (Feb. 16, 2016), https://www.eff.org/deeplinks/2016/02/eff-support-apple-encryption-battle. But specialized software created pursuant to a criminal investigation differs from a backdoor installed prior to purchase. The former is subject to procedural protections and requires the participation of a third party; the latter is subject to arguably weaker procedural protections and may be exploited without resort to the manufacturer.

[187] For a brief discussion comparing the function of encryption and physical means of data protection, see *The GNU Privacy Handbook*, THE FREE SOFTWARE FOUND. (1999), https://www.gnupg.org/gph/en/manual.html ("When a correspondent encrypts a document using a public key, that document is put in the safe, the safe shut, and the combination lock spun several times.").

[188] *See, e.g.*, DIE HARD (Gordon Company & Silver Pictures 1988) (highlighting a corporation's reliance on vaults despite vulnerability to third-party intrusion).

[189] *See infra* note 209 and accompanying text (discussing Fourth Amendment protections).

* * *

The foregoing analysis supports three observations. First, the marketplace-of-ideas theory and democratic self-governance theory of free speech, if taken seriously, do not protect source code used outside the realm of public dialogue. A programmer working alone or in a closed group[190] does not participate in the exchange of ideas, and their absence does not further the discovery of truth.[191] Nor does their work improve the effectiveness of democratic decision making.

Second, while the individual autonomy theory offers the best argument that encryption source code merits constitutional coverage, the theory itself proves too much. The First Amendment treats the creation of art and purely functional objects differently, though both may be "uniquely human."[192] Whereas the former expresses, the latter does not. And I assert that source code designed for the specific purpose of encrypting communications or circumventing such encryption, and without the expectation of peer review, more closely resembles a functional object than it does an expressive work.

Third, Robert Post's novel theory of free speech—which delimits First Amendment coverage according to the social context of communication—affords the most plausible rationale that encryption source code merits First Amendment coverage, though only to the extent that a regulation affects "the production and use of [regulated] software."[193] Therefore, a less intrusive regulation on "private," purely functional source code (like software designed to circumvent the encryption architecture on a single device) would more likely avoid First Amendment coverage than an expansive one (like a backdoor enabling access to all devices).

Having observed that no plausible normative theory of free speech requires constitutional coverage of all source code, I next consider whether likely governmental motives would trigger First Amendment scrutiny.

---

[190] I define a closed group as a group of programmers communicating among themselves for the completion of otherwise purely functional source code, but without the intention to use that source code with nonmembers.

[191] A caveat: An argument may be made that what would be considered purely functional source code could easily become expression source code active in public discourse by the addition of an annotation directed at another programmer. My definition of purely functional source code does not include code not intended for third-party review. *See supra* note 28 and accompanying text. The addition of a comment purportedly directed at another party does not make code non-purely functional unless the programmer has a sincere intent to convey information.

[192] Redish, *supra* note 155, at 628.

[193] Post, *supra* note 112, at 722.

B. Determining the Scope of Speech by Governmental Motive

An alternative, independent mode of distinguishing covered speech from nonspeech assesses the motives for regulation.[194] Applying this mode, courts invoke First Amendment scrutiny when the state acts for reasons inconsistent with the normative justifications for free speech, even if the communications are not otherwise covered.[195] For example, a court may strike a statute under the First Amendment when the state enacts a regulation "based on hostility—or favoritism—towards the underlying message expressed" by a speaker.[196] An ordinance restricting conduct to advance a noncensorial interest, meanwhile, would tend not to invoke such scrutiny unless the court deems such an interest illegitimate.[197]

Now consider the government's conduct after the San Bernardino terrorist attack. Recall that the Northern District of California issued an order requiring Apple to provide "reasonable technical assistance" in accessing the suspect's phone pursuant to an active criminal investigation.[198] In its appeal, Apple claimed the government acted with improper motive. By requiring Apple to compromise its security fea-

---

194 *See* Kagan, *supra* note 119, at 414 (arguing that "First Amendment law, as developed by the Supreme Court over the past several decades, has as its primary, though unstated, object the discovery of improper governmental motives"); Post, *supra* note 119, at 1255–56 (suggesting the "nature of the interests which the regulation services" constitutes one of two considerations that trigger First Amendment scrutiny and citing Texas v. Johnson, 491 U.S. 397, 406–07 (1989) ("It is . . . not simply the . . . nature of the expression, but the governmental interest at stake, that helps to determine whether a restriction on that expression is valid.")); Rubenfeld, *supra* note 167, at 775–78 (arguing the application of First Amendment law centers on ascertaining a law's purpose). *But see* Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445, 1478 (2013) (challenging this mode of analysis as "inconsistent with a significant number of Supreme Court cases that applied the First Amendment despite the fact that the underlying regulation had an economic motive").

195 Post, *supra* note 119, at 1276.

196 *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 386 (1992) (holding facially invalid a city ordinance prohibiting bias-motivated disorderly conduct). This type of regulation contradicts normative theories already discussed: the marketplace-of-ideas theory of the First Amendment emphasizes the importance of an open debate, *see supra* Section II.A.1; the individual autonomy theory emphasizes the importance of the individual to act as in a way that he pleases, *see supra* Section II.A.3. Note, then-Professor Elena Kagan uses *City of St. Paul* to explain how "a desire to punish impermissible purpose may explain and animate the Court's elaboration of doctrine." Kagan, *supra* note 119, at 416–23.

197 *See* Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 586 (1983) (holding a state may not use its interest in raising revenue to justify a special tax applied to publications protected by the First Amendment); *see also* Kagan, *supra* note 119, at 422 (discussing how a finding of neutral motivations influences the judges' approach in applying First Amendment law).

198 *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant, ED 15-0451M, at 2 (C.D. Cal. Feb. 16, 2016) (compelling Apple, Inc. to assist agents in search).

tures with specially designed software, Apple's argument went, the Bureau sought to compel speech: "The government asks this Court to command Apple to write software . . . [whose] code must contain a unique identifier . . . [and which] must be 'signed' cryptographically by Apple using its own proprietary encryption methods . . . . This amounts to compelled speech and viewpoint discrimination in violation of the First Amendment."[199]

In response, the government characterized the demand placed on Apple as a narrowly tailored means of completing a criminal investigation (apparently conceding to Apple's characterization of computer code as speech):

> It applies to a single iPhone, and it allows Apple to decide the least burdensome means of complying. As Apple well knows, the Order does not compel it to unlock other iPhones or to give the government a universal "master key" or "back door." It is a narrow, targeted order that will produce a narrow, targeted piece of software capable of running on just one iPhone, in the security of Apple's corporate headquarters.[200]

Under the framework explained above, a court would consider the application of First Amendment scrutiny according to whether the governmental motive threatened the normative rationales underlying the First Amendment. However, Apple's argument that the FBI targeted it because of its philosophy on privacy is not supported by the narrowness of the order, which demands access to a single device in a secure setting.[201] In order to accomplish such an objective, the government would have sought a more sweeping order implicating the security of all similar devices. Indeed, the extreme narrowness of the order in securing the contents of an encrypted device reflects a governmental interest not contrary to principles underlying the free speech doctrine.

---

[199] Apple Inc.'s Motion to Vacate, *supra* note 16, at 32 (internal quotations and citations omitted). Note that Apple made two claims under the First Amendment: first, that the government had sought to compel speech, and second, that the government had engaged in viewpoint discrimination because it disagreed with the value Apple placed on "data security and the privacy of citizens." *Id.* at 33. To the extent the second deals with the expression of a political opinion rather than purely functional source code, it is beyond the scope of this Note's thesis.

[200] Government's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant, CM 16-10 (Mar. 10, 2016) (noting national security interest implicated by a terrorism investigation).

[201] *See In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant, ED 15-0451M, at 2 (requiring software breaking Apple's privacy technologies be used at an Apple or government facility).

Compromising the encryption architectures of a single device does not threaten the vitality of public discourse except with regard to the suspect targeted.[202] Nor does it impinge on the general interest in promoting self-expression, if such an interest has any utility at all.[203] Similarly, a narrow order such as this does not threaten ancillary social considerations Post mentions in describing his theory of the First Amendment.[204] If the FBI had pursued a broader order endangering the security of all devices, a court might have answered differently.[205] The scope of the order here, however, does not implicate the speech interests of the consumer market.

CONCLUSION

Invoking freedom of speech provides lawyers with substantial rhetorical power: "The First Amendment not only attracts attention, but also strikes fear in the hearts of many who do not want to be seen as opposing the freedoms it enshrines."[206] For this reason, one scholar observes, many legal questions not obviously understood as implicating speech are framed nonetheless as First Amendment cases.[207] While this lawyering strategy serves the interests of the client, it strains the boundaries of the free speech doctrine. An expansion of our understanding of speech not justified by familiar theories used to explain the scope of the First Amendment dilutes its original meaning and undermines the normative bulwarks courts have used to explain its limits.

With this in mind, I return once more to the problem posed at the outset: Is purely functional source code speech covered by the First Amendment? Throughout this Note I have distinguished and have left to one side source code serving a purpose beyond communication

---

202 Recall that marketplace-of-ideas rationale aims to promote public dialogue. *See supra* Section II.A.1; *see also supra* Section II.A.2 (characterizing the democratic self-government theory as protecting discourse increasing voter knowledge and political sensitivity).

203 *See supra* Section II.A.3 (characterizing individual autonomy theory as valuing means of conduct that engages the mind).

204 *See supra* Section II.A.4 (hypothesizing that Post would consider a broad regulation more likely to implicate speech).

205 *See supra* notes 182–85 and accompanying text (explaining how judicial scrutiny of regulations may depend on the regulations' scope).

206 Schauer, *supra* note 29, at 1790.

207 Two examples: The treatment of homelessness has been cast as a speech issue (the right to beg), and the former military policy punishing the disclosure of one's sexual orientation had been framed as a free speech problem, when both could be framed as problems of equality. *See id.* at 1793–95 (describing how the First Amendment's potency may inspire lawyers to add to their claims a First Amendment challenge in the hope of increasing the likelihood of success).

with a computer. Whereas the latter may be entitled to coverage under the First Amendment—in part, because it may advance the science of cryptography—I argue the former does not because it serves no interest justifying the freedom of speech.

That such a genre of source code does not merit First Amendment protection is not a hypothetical legal issue. The government has sought to compel the creation of purely functional source code as recently as last year. And given the increasing ubiquity of the encryption architectures in storage devices and communications software,[208] the problem motivating this law enforcement technique—the "going dark" problem—will only intensify. If my conclusion is correct, the next court to confront this problem should carefully consider the manufacturer's resort to a First Amendment argument to resist the creation of functional source code, and ask whether a ruling in the manufacturer's favor truly serves the purpose of free speech.

While this Note forecloses one legal argument, nothing in these pages suggests a manufacturer must comply with a court order compelling the creation of software for law enforcement purposes. It removes only one ground for objection, leaving all others in place. Without a First Amendment argument, advocates for manufacturers' interests still may resort to the Fourth Amendment's privacy guarantee and the Fifth Amendment's privilege against self-incrimination.[209] If successful, these arguments would mitigate the industry's concerns for the consumers' security. But it also would advance another interest of greater theoretical salience—preserving the bounds of the First Amendment.

---

[208] *See supra* notes 4–5 (noting the amount of encrypted internet traffic and use of encryption on smart phones).

[209] *See generally, e.g.*, Folkinshteyn, *supra* note 20 (examining the application of the Fifth Amendment privilege against self-incrimination to compelled disclosure of unencrypted data); Dan Terzian, *Force Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 Nw. U. L. REV. ONLINE 56 (2014) (discussing the significance of the self-incrimination clause in the context of law enforcement investigations involving encrypted technologies); Wilson, *supra* note 20 (discussing the extent to which the Fourth and Fifth Amendments protect individuals when the government forces third parties to disclose passwords).