# CODE SPEAK: CONSTITUTIONAL AVOIDANCE ON THE FIRST AMENDMENT ENCRYPTION QUESTION*

## I. INTRODUCTION

On the morning of December 2, 2015, Syed Rizwan Farook attended a holiday party at his workplace, the Inland Regional Center for San Bernardino, California.[1] He "left abruptly" and "seemed angry."[2] He returned to work at 11:00 a.m. with his wife, Tashfeen Malik.[3] Armed with various firearms, the pair killed fourteen people and injured twenty-one.[4] They fled the scene, leaving three pipe bombs that they hoped would kill first responders.[5]

Authorities traced Farook and Malik to a nearby home the couple rented.[6] A firefight broke out, and both suspects were killed.[7] Authorities recovered Farook's iPhone from the scene.[8] The FBI hoped to glean information from the phone regarding the attack, including possible associates or co-conspirators.[9]

Due to the iPhone's advanced security features, however, it took months for the FBI to access the phone's data.[10] The primary reason was

[*] Brandon Matsnev, J.D. Candidate, Temple University Beasley School of Law, 2018. I want to thank, first and foremost, my family and friends for their unwavering support during my law school experience and beyond. Thanks also to the great editors of this fantastic journal, especially Kevin Trainer, Sonya Bishop, Sydney Pierce, and Cody Wolpert, whose time and dedication transformed this piece. Lastly, I want to thank Professor Robert Reinstein for his invaluable guidance both in writing this piece and in my professional endeavors.

[1] Krishnadev Calamur, Marina Koren & Matt Ford, *A Day After the San Bernardino Shooting*, ATLANTIC (updated Dec. 3, 2015, 3:08 PM), http://www.theatlantic.com/national/archive/2015/12/a-shooter-in-san-bernardino/418497/ [perma: http://perma.cc/NXZ3-MM3G].

[2] Saeed Ahmed, *Who Were Syed Rizwan Farook and Tashfeen Malik?*, CNN (updated Dec. 4, 2015, 7:23 PM), http://www.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/ [perma: http://perma.cc/R465-3U2Q].

[3] Calamur, Koren & Ford, *supra* note 1.

[4] *Id.*

[5] *Report Details Horror, Heroism During San Bernardino Shooting*, REUTERS (Sept. 10, 2016, 11:12 AM), http://www.reuters.com/article/us-california-shooting-idUSKCN11G0FI [perma: http://perma.cc/25TK-F3RK].

[6] Calamur, Koren & Ford, *supra* note 1.

[7] *Id.*

[8] *See* Laura Wagner, *FBI Paid More than $1 Million to Access San Bernardino Shooter's iPhone*, NPR: THE TWO-WAY (Apr. 21, 2016, 6:06 PM), http://www.npr.org/sections/thetwoway/2016/04/21/475175256/fbi-paid-more-than-1-million-to-access-san-bernardino-shooters-iphone [perma: http://perma.cc/C65N-RGEK].

[9] Mark Hosenball, *FBI Paid Under $1 Million to Unlock San Bernardino iPhone: Sources*, REUTERS (Apr. 28, 2016, 9:30 PM), http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032 [perma: http://perma.cc/Z3FH-W3M6].

[10] Chance Miller, *U.S. Judge Orders Apple to Help FBI Access Data on San Bernardino Gunman's iPhone 5c*, 9TO5MAC (Feb. 16, 2016, 5:11 PM), http://9to5mac.com/2016/02/16/u-s-judge-orders-apple-to-help-fbi-access-data-on-san-bernardino-gunmans-iphone-5c/ [perma: http://perma.cc/94GZ-YJM2].

encryption[11]—a function that scrambles a user's data, making it unreadable.[12] The Federal Government, unable to break the encryption on its own, requested a court order forcing Apple to rewrite its software to eliminate the security features on this specific phone.[13] The government based its request on the "All Writs Act,"[14] an arcane statute from 1789.[15] The court order was granted.[16] In its challenge to the order, Apple argued that being forced to write code was a violation of its First Amendment right to free speech.[17] The nation prepared for a titanic legal battle—"The Case of the Century"—that would shape the perennial debate between privacy and security for years to come.[18] But the battle never happened. The FBI paid an unknown entity almost $1 million to break into the iPhone and withdrew its request to the court.[19]

While one battle was never waged, the war between law enforcement and technology companies is escalating. After the case, Apple did not retreat. To the contrary, it vowed to enhance its already robust security measures.[20] Encryption is on the rise.[21] The technology community and law enforcement are on an inevitable collision course. Analyzing the legal battle arising out of the San Bernardino tragedy—specifically the All Writs Act and First Amendment arguments—may foreshadow what is to come. The converging issues of law enforcement, compelled computer code, and free speech are bound to come up again.

If these issues clash in federal litigation, a court should resolve them through the doctrine of constitutional avoidance, whereby a court steers clear of

[11] *Id.*

[12] *See* Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000).

[13] Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search at 6, 11, *In re* Search of an Apple iPhone, No. ED 16-10 (SP) (C.D. Cal. Feb. 19, 2016) [hereinafter Government's Motion to Compel].

[14] *Id.* at 7.

[15] Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 40–42 (1985) (describing origins of All Writs Act).

[16] *In re* Search of an Apple iPhone, No. ED 15–0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 1, 2016) (order compelling Apple to assist agents in search)

[17] Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 32, *In re* Search of an Apple iPhone, No. ED 16-10 (SP) (C.D. Cal. Feb. 25, 2016), http://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf [perma: http://perma.cc/CM9U-BRAM ] [hereinafter Apple's Brief].

[18] Jordan Orlando, *The Case of the Century*, SLATE (Feb. 25, 2016, 2:41 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2016/02/the_fbi_s_fight_with_apple_will_be_the_case_of_the_century.html [perma: http://perma.cc/CK47-SFAM].

[19] Hosenball, *supra* note 9.

[20] Joel Rubin, James Queally & Paresh Dave, *FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle with 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 [perma: http://perma.cc/J5YQ-XC2L].

[21] *See, e.g.*, Danny Yadron, *Facebook, Google, and WhatsApp Plan to Increase Encryption of User Data*, GUARDIAN (Mar. 14, 2016, 6:00 PM), http://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple [perma: http://perma.cc/3GS4-8UZ9].

adjudicating a constitutional matter when a plausible statutory interpretation exists.[22] The All Writs Act provides the statutory escape hatch for purposes of the constitutional avoidance doctrine. Where law enforcement seeks to force a technology company to draft code to circumvent encryption, a court should rule in favor of the technology company by interpreting the All Writs Act in a way that forbids this. Doing so will prevent judicial entanglement in a national debate that should be resolved legislatively. Ultimately, Congress should enact a new federal statutory regime that will balance privacy concerns on the one hand with national security and criminal justice concerns on the other.

## II. OVERVIEW

This Section provides the relevant technological and legal framework. Part II.A explains encryption, the iPhone's security system, the FBI's technology problem in San Bernardino, and past tension between law enforcement and advancing technology. Parts II.B and II.C provide an overview of the law, including the All Writs Act and the First Amendment, respectively. Part II.D discusses the canon of constitutional avoidance and its theoretical basis.

### A. *Technological and Historical Background: Encryption*

Computer technology has advanced greatly since its inception. Initially, users had to physically (and manually) modify a computer's hardware for the machine to perform a new task.[23] Technological advances eventually allowed users to store and use multiple programs without physically modifying the hardware each time a new task was to be completed.[24] These programs are called software, which is designed using computer code.[25] Thus, modern computers work by following instructions set out in computer code to execute programs.[26] Computer code is often referred to as "source code."[27] For a computer to execute the source code's commands in order to operate a program, the source code must first be converted into "object code."[28] Object code provides

[22] *See, e.g.*, Matthew E. Hedberg, Note, Kim Ho Ma v. Reno*: Cloaking Judicial Activism as Constitutional Avoidance*, 76 WASH. L. REV. 669, 670 (2001) (discussing use of constitutional avoidance in context of immigration law).

[23] Yvonne C. Ocrant, Comment, *A Constitutional Challenge to Encryption Export Regulations: Software Is Speechless*, 48 DEPAUL L. REV. 503, 505 (1998); *see also* Katherine A. Moerke, Note, *Free Speech to a Machine? Encryption Software Source Code Is Not Constitutionally Protected "Speech" Under the First Amendment*, 84 MINN. L. REV. 1007, 1045 (2000) (discussing the original development and programming of computers).

[24] Moerke, *supra* note 23, at 1045.

[25] *Id.*

[26] Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of YouTube, Facebook, and the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319, 327 (2012).

[27] 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 (2000).

[28] *Id.* at 143–44.

instructions to the computer in the form of 0s and 1s.[29] A compiler converts source code into object code, which a computer reads to execute the instructions set out in the source code.[30]

Enter encryption.[31] Encryption is the process of converting a message, or plaintext, into an unreadable scrambled text, or ciphertext.[32] Decryption, on the other hand, is the process of converting this scrambled text back into a readable message.[33] A "key" coverts plaintext into ciphertext and ciphertext back to plaintext.[34]

Computer programs can be designed to encrypt various forms of data, including personal messages and bank transactions.[35] Thus, when a message is run through this encryption software, it is converted into unreadable ciphertext according to an algorithm.[36] Encryption software also decrypts ciphertext back to plaintext with the right key, which unlocks the encoded message.[37] Encryption has traditionally been a government enterprise, often applied to protect military intelligence.[38] However, the rise of commercial computer technology has ushered in its civilian application.[39]

### 1. The iPhone's Security System

An iPhone's operating system (iOS) includes a function that encrypts the phone's sensitive data.[40] Only recently has Apple introduced encryption by

[29] Junger v. Daley, 209 F.3d 481, 483 (6th Cir. 2000). For example, source code might look like "Do x." However, when translated into object code for the computer to read and execute, it may look like "001010." *See id.*

[30] Ryan Christopher Fox, Comment, *Old Law and New Technology: The Problem of Computer Code and the First Amendment*, 49 UCLA L. REV. 871, 880 (2002).

[31] Encryption is "the best way to keep people from reading your emails short of making the subject line 'FWD:FWD:FWD:FWD Hilarious joke from Uncle Walter.'" *Last Week Tonight with John Oliver: Encryption* (HBO television broadcast Mar. 13, 2016).

[32] *Junger*, 209 F.3d at 482.

[33] Rod Dixon, *When Efforts to Conceal May Actually Reveal: Whether First Amendment Protection of Encryption Source Code and the Open Source Movement Support Re-Drawing the Constitutional Line Between First Amendment and Copyright*, COLUM. SCI. & TECH. L. REV., Sept. 28, 2000, at art. 2, 16 n.46.

[34] *Id.* at 19–20. For example, John wants to send Jack the following message: "HI." They want this message to be secret, so John creates a list of letters and corresponding numbers. "H" corresponds with "3" and "I" corresponds with "5." Thus, the message will read "35." This message, once translated to numbers, has been encrypted. The "key" is the list of letters and their corresponding numbers.

[35] Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1429 (N.D. Cal. 1996).

[36] *Id.*

[37] Moerke, *supra* note 23, at 1019.

[38] Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000).

[39] *See* Alex Colangelo & Alana Maurushat, *Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses, and Technological Protection Measures*, 51 MCGILL L.J. 47, 73 (2006).

[40] Matthew Green, *Is Apple Picking a Fight with the U.S. Government? Not Exactly.*, SLATE (Sept. 23, 2014, 10:51 AM), http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html [perma: http://

default.[41] Here is how encryption works. Every iPhone has a unique number called an encryption key.[42] Without the key, any encrypted data will be incomprehensible. The encryption key to the iPhone will unscramble the data; however, the key has many trillion possible values, making it essentially impossible for a hacker to access the iPhone's data by guessing the key.[43] Every single iPhone has an individualized encryption key, but Apple does not store these keys anywhere.[44]

An iPhone user automatically encrypts her iPhone when she sets a passcode, a number that by default is only four or six digits long.[45] The passcode the user chooses is integrated into the encryption key.[46] Entering the passcode essentially unlocks the data by "completing" the key.[47] A passcode, unlike the entire encryption key, only has 10,000 possible values if the four-digit option is chosen.[48] This means it is easier to guess the passcode than the entire encryption key, which, ironically, makes the passcode the weakest part of the iPhone's security system.[49]

Hypothetically, a person wishing to access a phone's data could guess until he got the passcode right. Apple, however, has two security features to prevent that possibility.[50] First, after four failed attempts, a time delay is introduced, forcing a user to wait to try again.[51] The length of this delay increases with every failed attempt.[52] Second, the user has the option to enable a setting that automatically wipes all the iPhone's data after ten failed tries.[53]

perma.cc/7U52-G5KX].

[41] Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC NEWS (Sept. 19, 2014), http://www.bbc.com/news/technology-29276955 [perma: http://perma.cc/634D-UTVD] [hereinafter Miller, *Google and Apple*].

[42] Timothy B. Lee, *Apple's Battle with the FBI over iPhone Security, Explained*, VOX (Feb. 17, 2016, 3:50 PM), http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino [perma: http://perma.cc/CPL6-CWDX] [hereinafter Lee, *Apple's Battle Explained*].

[43] *Id.*

[44] *Id.*

[45] APPLE, INC., IOS SECURITY: IOS 11, at 12 (2018), http://www.apple.com/business/docs/iOS_Security_Guide.pdf [perma: http://perma.cc/2FKS-VL3P].

[46] *Id.*

[47] *See id.*

[48] *Id.*

[49] *Id.* To illustrate, suppose the manufactured encryption key that comes with one particular iPhone is as follows: "1_3_5." Suppose the passcode is two digits, and the phone's user selects "24." The key becomes "12345." Entering the passcode, then, "completes" the key and unscrambles all the phone's data. An individual trying to access the phone's data need not guess "1_3_5" to unlock the phone. He simply needs to guess the passcode, "24," correctly.

[50] Micah Lee, *Upgrade Your iPhone Passcode to Defeat the FBI's Backdoor Strategy*, INTERCEPT (Feb. 18, 2016, 4:05 PM), http://theintercept.com/2016/02/18/passcodes-that-can-defeat-fbi-ios-backdoor/ [perma: http://perma.cc/WT82-9SQW] [hereinafter Lee, *Upgrade Your iPhone*].

[51] *Id.*

[52] *Id.*

[53] *Id.*

### 2. The Technology Problem in San Bernardino

Following the San Bernardino attack, the FBI found an iPhone belonging to one of the suspects.[54] The FBI wanted to access the phone to see if it contained any helpful information about the attack.[55] However, the phone was locked behind a passcode.[56] The Bureau did not want to attempt to guess the passcode, since it had reason to believe the suspect enabled the setting that would erase the phone's data after ten tries.[57] Nor could it remove the data from the phone because the encrypted data would be incomprehensible without the passcode to unscramble it.[58] So, the FBI requested a court order to compel Apple to create new software that would eliminate the security features—the automatic data wipe and the time delays—preventing the FBI from accessing the suspect's data.[59] The FBI could not use its own software to access the iPhone's data because iPhones only operate software that has been digitally signed by Apple.[60] Essentially, the FBI wanted "a customized version of iOS," or a "backdoor" to the iPhone.[61]

### 3. Law Enforcement, Encryption, and Backdoors: Past and Future

The concept of a backdoor is not new. In 1993, the Clinton Administration, fearful of private encryption, introduced government-provided encryption technology known as the "Clipper Chip."[62] Essentially, the government proposed an encryption system for technology companies to use, to which only the government had decryption capabilities.[63] The government would implement

[54] Hosenball, *supra* note 9.

[55] *Id.*

[56] *See id.*; Lee, *Apple's Battle Explained*, *supra* note 42.

[57] Joel Rubin & Paresh Dave, *FBI Says It Might Be Able to Unlock San Bernardino Terrorist's iPhone Without Apple's Help*, L.A. TIMES (Mar. 21, 2016, 8:35 PM), http://www.latimes.com/local/lanow/la-me-ln-feds-looking-at-another-way-to-unlock-terror-attacker-s-iphone-seek-delay-in-hearing-20160321-story.html [perma: http://perma.cc/58ET-S8VV].

[58] *See* Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000).

[59] *See* Government's Motion to Compel, *supra* note 13, at 2.

[60] *Id.* at 11.

[61] Damon Beres, *What You Need to Know About Apple vs. the FBI*, HUFFINGTON POST (Feb. 19, 2016, 7:59 AM), http://www.huffingtonpost.com/entry/apple-vs-fbi-explainer_us_56c5d5d0e4b0c3c55053e130 [perma: http://perma.cc/4C3U-HECH]. In its brief, Apple expressed concern about being technologically stuck between a rock and a hard place if the government's motion succeeded. Apple's Brief, *supra* note 17, at 24. If Apple destroyed the code after writing it, it would have to rewrite code every single time law enforcement needed to access an iPhone. *Id.* If it kept the code, it would have to go to extraordinary measures to protect the code from exploitation by hackers. *Id.*

[62] This was announced via press release from the White House. *See* Press Release, White House, Office of the Press Sec'y, Statement by the Press Sec'y (Apr. 16, 1993).

[63] *Id.* at 2 ("Access to [this technology] will be limited to government officials with legal authorization to conduct a wiretap."). The proposal reflected law enforcement's concern that it was gradually losing access to data and its fears of being unable to perform its duties given the growth of strong encryption. *See* Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES MAG. (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-

the program, first, by inserting the chip into phones used by government agencies. The program would later expand to commercial telephone and computer networks.[64] Law enforcement could access the data via a "key-escrow," which meant that government agencies would actually hold encryption keys in storage.[65] When an agency required access to an encrypted phone, pursuant to a warrant, the agency would request a key to unlock the data.[66] Technology companies and privacy advocates were alarmed. This showdown was called the "first holy war of the information highway."[67] That war, however, was never waged, as a hacker discovered a vulnerability in the Clipper Chip.[68]

As recently as 2010, the encryption war raged on, as the Obama administration sought to submit a bill that would have required technology companies to remain "technically capable" of complying with court orders.[69] This would have meant redesigning their technology to allow for interception of communications and decryption of data.[70] The FBI framed it not as an expansion of its authority but as a preservation of its ability to enforce the law in the face of advanced encryption technology.[71]

In some ways, then, the FBI's confrontation with Apple over San Bernardino appeared as just another battle in the larger war. It was unique in one respect, however, in that it was the first time a technology company was compelled, via court order, to draft code for the government.[72] The FBI based its

chip.html?pagewanted=all&mcubz=1 [perma: http://perma.cc/5EDW-EZLQ]; *see also* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 744 (1995) ("[T]he intelligence agencies, primarily the NSA, quietly murmur that existing policies have proved ineffective in preventing the increasing use of unescrowed encryption, and suggest that their proposals should be adopted to prevent developments that might (or might not, they won't say) undermine the nation's communications intelligence capabilities.").

[64] John Markoff, *Electronics Plan Aims to Balance Government Access with Privacy*, N.Y. TIMES (Apr. 16, 1993), http://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html [perma: http://perma.cc/S6EB-CWW9].

[65] *See* Press Release, White House, *supra* note 62.

[66] *Id.*

[67] Levy, *supra* note 63.

[68] *See* Matt Blaze, *A Key Under the Doormat Isn't Safe. Neither Is an Encryption Backdoor.*, WASH. POST (Dec. 15, 2015), http://www.washingtonpost.com/news/in-theory/wp/2015/12/15/how-the-nsa-tried-to-build-safe-encryption-but-failed/?utm_term=.e03fad17ce4d [perma: http://perma.cc/JL2T-22RW].

[69] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=0 [perma: http://perma.cc/D29C-7UYH]. The administration ultimately backed down from the proposal. Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0 [perma: http://perma.cc/QYA5-XC62].

[70] Lichtblau & Benner, *supra* note 69.

[71] *Id.*

[72] Apple was previously able to extract data from users' iPhones easily because the data was not encrypted. *See* Christie Smythe, *How Apple Helped Me Crack iPhones Like Clockwork*, SYDNEY MORNING HERALD (Mar. 17, 2016), http://www.smh.com.au/business/world-business/how-apple-helped-me-crack-iphones-like-clockwork-20160316-gnl1uc.html [perma: http://perma.cc/9G5J-GCSC].

entire argument on a little-known statute, the All Writs Act of 1789.[73] And Apple responded with a free speech defense, among other arguments, asserting it was being compelled to speak in violation of the First Amendment.[74]

Like the Clipper Chip controversy from the early 1990s, the San Bernardino battle was never waged; the FBI circumvented Apple's encryption technology.[75] Understanding the law at issue, though, will allow us to anticipate the next events of the encryption war and, perhaps, predict the eventual outcome.

### *B. The All Writs Act*

The All Writs Act (the Act) provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[76] The Act fills a gap by allowing a court to issue an injunction when an alternative remedy is lacking.[77] Courts rarely use the Act,[78] but when they do, the purpose is typically to aid in the investigation of the facts of a case.[79]

In applying the ambiguous language of the Act, courts do not interpret the term "necessary" in an absolute sense.[80] The term simply requires that issuance of a writ is "calculated . . . in [a court's] sound judgment to achieve the ends of justice" and the "rational ends of law."[81] Additionally, "in aid of their respective jurisdictions" means that the Act does not create substantive jurisdiction on its own—it is a codification of the federal courts' power to protect the jurisdiction they already have.[82]

[73] *See* Government's Motion to Compel, *supra* note 13, at 6, 11.

[74] *See* Apple's Brief, *supra* note 17, at 32.

[75] Rubin & Dave, *supra* note 57.

[76] All Writs Act §§ 234, 261, 262, 28 U.S.C. § 1651(a) (2012). The current language is the result of a reorganization of the Act in 1948. Paul R. Gugliuzza, *The New Federal Circuit Mandamus*, 45 IND. L. REV. 343, 354 (2012).

[77] *See* Dimitri D. Portnoi, Note, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in the Rights of Enemy Combatants*, 83 N.Y.U. L. REV. 293, 294 (2008).

[78] *Id.* at 295. One of the few illustrations of courts' use of the Act is the habeas case *Price v. Johnston*, 334 U.S. 266 (1948). Here, the Supreme Court found that, under the All Writs Act, an appellate court could "command that a prisoner be brought before it so that he may argue his own appeal in a case involving his life or liberty." *Id.* at 278. In *Johnston*, a prisoner petitioned for a writ of habeas corpus. *Id.* at 270. It was his fourth attempt to petition the court, and the trial court rejected it. *Id.* at 275–76. The prisoner appealed. *Id.* at 276. He declined the assistance of counsel and requested a court order directing that he be present for oral argument. *Id.* The Supreme Court found that it was within the appellate court's power to issue a writ directing the prisoner to appear. *Id.* at 278. The Court said that where exceptional circumstances are present, fairness to the prisoner requires that he be allowed to participate in oral arguments. *Id.* at 280.

[79] Harris v. Nelson, 394 U.S. 286, 299 (1969).

[80] Adams v. United States *ex rel.* McCann, 317 U.S. 269, 273 (1942).

[81] *Id.*

[82] *See* Klay v. United Healthgroup, Inc., 376 F.3d 1092, 1099 (11th Cir. 2004); Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979); Joan Steinman, *The Newest Frontier of Judicial Activism: Removal Under the All Writs Act*, 80 B.U. L. REV. 773, 779 (2000) ("[T]he Act cannot be used to legitimate the filing of original actions in federal court.").

### 1. Application to Third Parties Pre-1977

Before 1977, there was no clear standard regarding the issuance of writs under the All Writs Act to those not party to the litigation.[83] In some cases, courts determined that a third party's compelled participation was necessary to provide an adequate inquiry into a set of facts.[84] Thus, the Act can supply a court with instruments required to perform its duty.[85] Courts also issued the writ to third parties to prevent their lawful orders and judgments "from being thwarted and interfered with by force, guile, or otherwise."[86] *Harris v. Nelson*[87] and *Mississippi Valley Barge Line Co. v. United States*[88] supply two examples of the very few pre-1977 applications of the Act to third parties, and they do not demonstrate a uniform, cognizable rule for federal courts.[89]

### 2. The Post-1977 Framework

The 1977 case *United States v. New York Telephone Co.*[90] finally created a framework within which courts could apply the All Writs Act to third parties.[91] In this case, the Government believed the defendant was engaged in an illegal gambling operation.[92] It requested a court order compelling a telephone company—a third party—to provide certain technical assistance in installing a

[83] One court acknowledged that, given the wide variety of concerns previous cases applying the Act have addressed, "it is unclear how those traditional standards would even be applicable." *Klay*, 376 F.3d at 1102. Over the past 150 years, courts have not shown "the kind of precision or specificity which would make issuance of the writs a mechanical exercise." Morrow v. District of Columbia, 417 F.2d 728, 736 (D.C. Cir. 1969); *see also* Portnoi, *supra* note 77, at 295 ("[A] clear standard is lacking on the face of the statute.").

[84] *See, e.g.*, *Harris*, 394 U.S. at 300–01.

[85] *See id.* at 299–300.

[86] Miss. Valley Barge Line Co. v. United States, 273 F. Supp. 1, 6 (E.D. Mo. 1967), *aff'd mem.*, 389 U.S. 579 (1968).

[87] 394 U.S. 286 (1969).

[88] 273 F. Supp. 1 (E.D. Mo. 1967), *aff'd mem.*, 389 U.S. 579 (1968).

[89] In *Harris v. Nelson*, the Supreme Court issued a writ compelling a prison warden to answer interrogatories in connection with a prisoner's habeas corpus proceeding. *Id.* at 300. The prison warden was neither technically a third party, nor was he necessarily an adverse party. *Id.* at 296. The prisoner believed that the information leading to his conviction was improperly provided by an unreliable source. *Id.* at 288–89. The warden objected to the interrogatories, arguing that the Federal Rules of Civil Procedure did not provide for these discovery proceedings. *Id.* at 289. The Court used the Act to fill this gap. *Id.* at 290. The Court stated that, given the legitimacy of the prisoner's claims, discovery was necessary to facilitate an adequate inquiry into the facts. *Id.* at 300. *Mississippi Valley Barge Line Co. v. United States* concerned an individual's attempt to circumvent a court's decree and an order from a government commission. *Id.* at 6. The individual was not a party to the original action. *Id.* The court did not consider this fact to be relevant. *Id.* The individual was employing "subterfuge" and "deceptive and deceitful tactics" in order to frustrate compliance with the order. *Id.* at 3–6. The court determined that without an injunction against him, there would be irreparable injury to the plaintiff as well as to "this court's integrity and the judicial process of the United States of America." *Id.* at 6. It issued the injunction under the Act. *Id.* at 7.

[90] 434 U.S. 159 (1977).

[91] *N.Y. Tel. Co.*, 434 U.S. at 174–75.

[92] *Id.* at 162.

pen register (a type of call-tracking device) on one of the telephone company's phone lines.[93] The court order required the company to lease unused phone lines to the FBI, in order to install the register in an unobtrusive manner.[94] The company agreed to provide minor support, including identifying locations where the registers could be installed, but it refused to lease the lines.[95] The Supreme Court determined that the court order was proper under the All Writs Act and compelled the company to lease the lines.[96] The Court emphasized the flexibility of the Act, citing, among other cases, *Price v. Johnston*[97] and *Harris v. Nelson*.[98] It stated:

> [t]he power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice . . . and encompasses even those who have not taken any affirmative action to hinder justice.[99]

The Court concluded that the order was valid through three principal observations. First, the telephone company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled."[100] Second, the order was not "burdensome."[101] Third, without the company's help, there was "no conceivable way" the surveillance could have been accomplished.[102] In laying out these factors, the Court dismissed the lower court's concern that third-party writs under the Act would "establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impress unwilling aid on private third parties."[103]

#### *a.* New York Telephone *Set a Precedent*

Many courts have applied the three-factor *New York Telephone* framework to affirm third-party writs.[104] In 1980, the Ninth Circuit faced a similar set of facts in *United States v. Mountain States Telephone & Telegraph Co.*[105] and applied

[93] *Id.*

[94] *Id.*

[95] *Id.* at 162–63.

[96] *Id.* at 172.

[97] 334 U.S. 266 (1948), *overruled on other grounds by* McClesky v. Zant, 499 U.S. 467 (1991).

[98] *N.Y. Tel. Co.*, 434 U.S. at 172–73.

[99] *Id.* at 174.

[100] *Id.*

[101] *Id.* at 175.

[102] *Id.*

[103] *Id.* at 164 (quoting Application of United States *in re* Order Authorizing Use of a Pen Register, 538 F.2d 956, 962 (2d Cir. 1976), *rev'd*, *N.Y. Tel. Co.*, 434 U.S. 159).

[104] *See infra* notes 105–20 and accompanying text.

[105] United States v. Mountain States Tel. & Tel. Co. (*In re* Application of United States for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities), 616 F.2d 1122 (9th Cir. 1980) [hereinafter *Mountain Bell*].

*New York Telephone* to resolve its case.[106] The government had probable cause that a suspect was gambling illegally and requested an order compelling the Mountain Bell Telephone Company to install a "grabber," a call-tracking device more advanced than the pen register, on one of the company's telephone lines.[107] The government needed a grabber, rather than a pen register, because the telephone company's call-routing utilities were more advanced than those used in *New York Telephone*.[108] A major difference between the use of these devices was that the pen register could be used remotely by law enforcement and required little assistance from the telephone company.[109] The grabber, on the other hand, had to be "activated by the programming of a computer by a technician of" Mountain Bell.[110]

Applying the *New York Telephone* test, the court disagreed that the programmer's work was an unreasonable burden and called the distinctions between the devices a "distinction without a difference."[111] Given the similarity between the cases coupled with the more enhanced necessity of the company's compliance, the court found that the test established in *New York Telephone* resolved the matter.[112] The All Writs Act could be used to require the company to install the grabber.[113]

In *United States v. Hall*,[114] the government, relying on the All Writs Act, forced a credit card company to produce the credit card records of a fugitive's associate to aid in finding the fugitive.[115] The court employed the three-factor test outlined in *New York Telephone* and came to the following conclusions.[116] First, the credit card company was not too far removed from the underlying action because its services facilitated illegal activity in a similar manner to a telephone company.[117] Second, the credit card company did not face an undue burden because it already compiled a monthly list of all purchases for each customer in advance of payment.[118] Third, while absolute necessity was not present because there was more than one way to catch the fugitive, the credit card company's service would have "materially assist[ed] in the apprehension" of the suspect and "facilitate[d] efforts to find" him.[119] For these reasons, the third element was met, and the credit card company was required to provide the

[106] *Mountain Bell*, 616 F.2d at 1128–30.

[107] *Id.* at 1123–24.

[108] *See id.* at 1127.

[109] *Id.*

[110] *Id.*

[111] *Id.* at 1130.

[112] *Id.* at 1129–30.

[113] *Id.* at 1132.

[114] 583 F. Supp. 717 (E.D. Va. 1984).

[115] *See Hall*, 583 F. Supp. at 719, 722.

[116] *Id.* at 719.

[117] *Id.* at 720.

[118] *Id.* at 721.

[119] *Id.* at 722.

individual's records to the government.[120]

### *b. Recent Cases*

In recent years, courts have varied widely in their application of the All Writs Act to force third-party companies like Apple to decrypt cell phones for law enforcement.[121] In 2014, a magistrate judge evaluated the government's request to require a phone manufacturer[122] to provide reasonable technical assistance by attempting to unlock one of its phones that may have contained evidence related to credit card fraud.[123] The government's request was based entirely on the All Writs Act.[124] In granting the request, the court compared the manufacturer's unlocking the phone to the installation of a pen register in *New York Telephone*, and found that this order would be appropriate.[125] It allowed the manufacturer to challenge the order to the extent that it would be unreasonably burdensome.[126] However, the court stated that "[c]ase law reflects that orders providing technical assistance of the kind sought here are often not deemed to be burdensome."[127]

A year later in 2015, a second magistrate judge, Judge Orenstein of New York, came out the other way.[128] Confronted with similar facts—the government required Apple's assistance in disabling the security of a suspected drug dealer's seized iPhone—Judge Orenstein was concerned that Apple would face an unreasonable burden.[129] The judge distinguished *New York Telephone* on various grounds. Instead of immediately denying the government's request, the

[120] *Id.* Courts have also applied *New York Telephone* to issue writs to third parties but have not explicitly utilized its three-factor analysis. *See, e.g.*, *In re* Application of United States of America for Order Directing X to Provide Access to Videotapes, Misc. No. 03-89, 2003 U.S. Dist. LEXIS 15227, at *8 (D. Md. Aug. 22, 2003) (requiring an apartment complex to provide access to surveillance tapes to help locate the defendant).

[121] See *infra* notes 122–45 and accompanying text for a discussion of this variation.

[122] The manufacturer was probably Apple, though this has never been confirmed. *See* Matt Zapotosky, *The Justice Department Said Tech Companies Have Accessed Phones for It Before. So the ACLU Tried to Find All the Cases*, WASH. POST: POST NATION (Mar. 30, 2016), http://www.washingtonpost.com/news/post-nation/wp/2016/03/30/the-justice-department-said-tech-companies-have-accessed-phones-for-it-before-so-the-aclu-tried-to-find-all-the-cases/?utm_term=.ad6d6783c32e [perma: http://perma.cc/23EL-TP3H] (ascribing manufacture in this case to Apple); *see also* Cyrus Farivar, *Feds Want Apple's Help to Defeat Encrypted Phones, New Legal Case Shows*, ARSTECHNICA (Dec. 1, 2014, 9:00 AM), http://arstechnica.com/tech-policy/2014/12/feds-want-apples-help-to-defeat-encrypted-phones-new-legal-case-shows/ [perma: http://perma.cc/4MQU-CWKG] (noting one phone manufacturer is "definitively Apple").

[123] *In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone, 14 Mag. 2258, 2014 U.S. Dist. LEXIS 154743, at *1 (S.D.N.Y. Oct. 31, 2014).

[124] *Id.*

[125] *Id.* at *3.

[126] *Id.* at *5.

[127] *Id.* at *4.

[128] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 15 MISC 1902, 2015 U.S. Dist. LEXIS 138755, at *17 (E.D.N.Y. Oct. 9, 2015).

[129] *Id.* at *19.

judge deferred to allow for oral argument.[130]

After each side presented its case, Judge Orenstein denied the government's request.[131] The judge presented an in-depth analysis of the three factors outlined in *New York Telephone*—closeness, degree of burden, and necessity of assistance.[132] First, the judge determined that Apple was too far removed from the investigation.[133] Unlike the gambler in *New York Telephone* who depended on the telephone company's lines, the suspect here used his own property in committing crimes.[134] The judge also rejected the government's argument that Apple was thwarting the investigation, stating that Apple was "not doing anything to keep law enforcement agents from conducting their investigation" or "conspir[ing] with [the suspect]."[135]

Second, the judge determined that Apple would have faced an unreasonable burden had it complied with the government's demand.[136] Apple does not, after all, ordinarily bypass its security in the course of business.[137] Additionally, circumventing its own security would undermine its position as an industry leader in security.[138] Compliance would also have required both extensive labor and hardware that do not constitute "minimal effort" as was the case in *New York Telephone*.[139] Regarding the third *New York Telephone* factor, the judge concluded that government had not made a persuasive argument that it could not access the phone without Apple's help.[140]

In the same month that Judge Orenstein issued his decision, Judge Pym of California came to the opposite conclusion, granting the FBI's request for Apple to provide assistance in unlocking the San Bernardino shooter's iPhone.[141] Apple's technical assistance may have included "providing the FBI with a signed iPhone Software file"—a backdoor to encryption.[142] The software's functionality was to be coded with a "unique identifier" to the subject's phone, which meant the FBI could not use it to unlock other phones.[143] Judge Pym's order did not discuss *New York Telephone*, nor did it analyze the case law that has developed under the All Writs Act.

In a motion to vacate, Apple presented a novel First Amendment defense

[130] *Id.* at *10–18.

[131] *In re* Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016) [hereinafter *Apple New York Case*].

[132] *Id.* at 364–75.

[133] *Id.* at 364.

[134] *Id.*

[135] *Id.* at 366.

[136] *Id.* at 369–70.

[137] *Id.* at 369.

[138] *Id.*

[139] *Id.* at 370 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 175 (1977)).

[140] *Id.* at 374–75.

[141] *In re* Search of an Apple iPhone, No. ED 15–0451M, 2016 U.S. Dist. LEXIS 20543, at *1–2 (C.D. Cal. Feb. 16, 2016) [hereinafter *Apple San Bernardino Case*].

[142] *See id.* at *2.

[143] *Id.* at *2–3.

to the All Writs Act.[144] It argued that being forced to write computer code is compelled speech in violation of the First Amendment.[145]

### *C. First Amendment*

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech."[146] First Amendment challenges often occur in the context of a law that prohibits or regulates certain speech.[147] However, First Amendment challenges also can arise in cases in which a party is being compelled to speak.[148] This Part will discuss compelled speech doctrine, beginning with general concepts and concluding with the issue of First Amendment coverage of computer code.

#### 1. Compelled Speech Generally

While the First Amendment often prohibits certain regulations on speech, it also forbids the government from forcing people to speak.[149] Compelled speech does not always warrant the same constitutional scrutiny as prohibited speech.[150] If a government action compelling speech is assessed under intermediate scrutiny, the compelled speech is constitutional only if "it furthers an important or substantial governmental interest . . . unrelated to the suppression of free expression," and if the restrictions on First Amendment rights are "no greater than is essential to the furtherance of that interest."[151] Under strict scrutiny, however, the government's law or action must be "narrowly tailored" to serve a "compelling state interest."[152]

Determining which test applies in a First Amendment analysis for compelled speech[153] begins with whether the compelled speech is content neutral

[144] *See* Apple's Brief, *supra* note 17, at 32.

[145] *Id.*

[146] U.S. CONST. amend. I.

[147] *See, e.g.*, Burson v. Freeman, 504 U.S. 191 (1992) (addressing state statute that prohibited the display and distribution of campaign materials within 100 feet of a polling place); Ward v. Rock Against Racism, 491 U.S. 781 (1989) (addressing city ordinance regulating the volume of music in an amphitheater adjacent to a designed quiet area).

[148] *See* Rumsfeld v. Forum for Acad. & Institutional Rights, Inc., 547 U.S. 47, 61 (2006) (recognizing that freedom of speech prohibits the government from telling people what they must say); Wooley v. Maynard, 430 U.S. 705, 713 (1977) (finding that a New Hampshire law that prohibited covering of the state's motto on its license plates violated of the First Amendment).

[149] *Forum for Acad.*, 547 U.S. at 61. A government that "secures the right to proselytize religious, political, and ideological causes must also guarantee the concomitant right to decline to foster such concepts." *Wooley*, 430 U.S. at 714.

[150] Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 637 (1994).

[151] *Id.* at 662 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[152] Frudden v. Pilling, 742 F.3d 1199, 1207 (9th Cir. 2014) (quoting Rounds v. Or. State Bd. of Higher Educ., 166 F.3d 1032, 1038 n.4 (9th Cir. 1999) (quoting Pac. Gas & Elec. Co. v. Public Utils. Comm'n, 475 U.S. 1, 19 (1986))).

[153] Courts treat compelled speech and compelled silence as constitutional equivalents. Riley v. Nat'l Fed'n of the Blind of N.C., 487 U.S. 781, 797 (1988).

or content based.[154] The former warrants intermediate scrutiny.[155] The latter triggers strict scrutiny.[156] This is determination is not easy, and there is no universal test for it.[157]

### *a. Content-Neutral Restrictions*

Laws that compel speech without regard to the substantive views expressed are generally deemed content neutral.[158] The reason content-neutral restrictions warrant a lesser standard of scrutiny is that courts are less concerned that the government is targeting a particular idea or viewpoint.[159] Often, the reason the government has adopted a particular regulation or imposed a burden on speech is dispositive in the content-neutrality question.[160] However, a determination that restrictions are content neutral on their face does not end the analysis, as some may be implicitly content based.[161]

*Turner Broadcasting System, Inc. v. FCC*[162] demonstrates the content-neutrality analysis—determine whether the restriction on speech is content based, and then apply the appropriate level of scrutiny.[163] The Cable Television Consumer Protection and Competition Act of 1992 required cable providers to broadcast local television stations.[164] This was known as a "must-carry" provision.[165] Cable operators sued, arguing that this provision violated the First Amendment.[166] The Court determined that the must-carry provisions were content neutral.[167] While these provisions "compell[ed operators] to offer carriage to a certain minimum number of broadcast stations," this burden was imposed on all operators, regardless of the programming each one offered individually.[168] So, the Act did not impose a burden or penalty based on the cable operator's views.[169] Further, the Court stated that the regulations were

[154] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 328 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[155] *Id.* at 327–28.

[156] *Id.* at 327; *see also* Leslie Gielow Jacobs, *Clarifying the Content-Based/Content Neutral and Content/Viewpoint Determinations*, 34 MCGEORGE L. REV. 595, 598 (2003).

[157] Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994); *see also* Jacobs, *supra* note 156, at 596 (explaining that the test remains "murky").

[158] *See Turner Broad. Sys.*, 512 U.S. at 643.

[159] Frudden v. Pilling, 742 F.3d 1199, 1207 n.5 (9th Cir. 2014); *see also* Colangelo & Maurushat, *supra* note 38, at 53 ("The prevalent view of free speech in the United States is that the government is not the appropriate authority to act as a censor and has, therefore, adopted the most permissive free speech legal framework.").

[160] *Turner Broad. Sys.*, 512 U.S. at 642–43.

[161] *Id.*

[162] 512 U.S. 622 (1994).

[163] *Turner Broad. Sys.*, 512 U.S. at 643, 661.

[164] *Id.* at 626.

[165] *Id.* at 630.

[166] *Id.* at 634–35.

[167] *Id.* at 643–44.

[168] *Id.* at 644.

[169] *Id.*

implemented with a neutral purpose—to increase free access to consumers—that was unrelated to the content of the cable or broadcast provider's views.[170]

Because the Court deemed the regulation content neutral, it evaluated the law using intermediate scrutiny.[171] The Court found the government interests to be substantial—preserving free broadcast television, promoting the spread of information from a variety of sources, and promoting fair competition among providers.[172] It then stated that tailoring to achieve these objectives would be satisfied if the incidental restriction on free speech rights is (1) "no greater than is essential to the furtherance of that interest,"[173] and (2) if the interest would be achieved "less effectively absent the regulation."[174] The Court found that the government did not demonstrate that these requirements were met.[175]

### *b. Content-Based Restrictions*

While courts have labeled various laws as content based, their holdings do not reveal any clear, universal rule for making this determination. In some circumstances, compelled speech is content based where the government requires a person to say something he otherwise would not.[176] The question can also turn on ideology: when the state seeks to advance a certain ideology, "such [a state] interest cannot outweigh an individual's First Amendment right to avoid becoming the courier for such message."[177] Neither can the government force the endorsement of a particular viewpoint.[178] However, the right against compelled speech is not limited to purely ideological messages and can extend to factual speech.[179] The two cases that follow demonstrate how the Supreme Court has applied strict scrutiny in compelled speech cases.

*Miami Herald Publishing Co. v. Tornillo*[180] principally concerned freedom of the press, but it had freedom of speech elements and is often relied upon in

[170] *Id.* at 646–47.

[171] *Id.* at 661–62.

[172] *Id.* at 662–63.

[173] *Id.* at 662 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[174] *Id.* at 662 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)).

[175] *Id.* at 667–68. It cited, among other indications, the absence of proof that broadcast stations were disappearing or suffering financial difficulties, which called into question the need for this legislation. *Id.*

[176] Riley v. Nat'l Fed'n of the Blind of N.C., 487 U.S. 781, 795 (1988). There is a class of cases dealing with content-neutral "commercial speech." These cases often evaluate regulations pertaining to advertising and product promotion. *See, e.g.*, United States v. United Foods, Inc., 533 U.S. 405 (2001). Per *United Foods*, the definition of commercial speech is "speech that does no more than propose a commercial transaction." *Id.* at 409. Discussing these cases would be outside the scope of this Comment since computer code does not necessarily propose a commercial transaction.

[177] Wooley v. Maynard, 430 U.S. 705, 717 (1977).

[178] *See* Frudden v. Pilling, 742 F.3d 1199, 1207 (9th Cir. 2014); *see also Wooley*, 430 U.S. at 721 (Rehnquist, J., dissenting) ("[T]he test [for content-based restrictions] is whether the individual is forced 'to be an instrument for fostering public adherence to an ideological point of view he finds unacceptable.'" (quoting *Wooley*, 430 U.S. at 715 (majority opinion))).

[179] *Frudden*, 742 F.3d at 1206.

[180] 418 U.S. 241 (1974).

freedom of speech cases.[181] Under a Florida "right of reply" statute, which forced a newspaper to publish a political candidate's response to criticism, a political candidate sued a newspaper that refused to dedicate space for him to respond.[182] The newspaper argued the statute violated the First Amendment because it essentially compelled newspapers to speak by forcing the publication of candidates' replies.[183] The Court agreed, finding the statute unconstitutional and rejecting the candidate's argument that newspapers should be regulated because of their near monopoly on information.[184] It also concluded that the statute "exact[ed] a penalty on the basis of the *content* of a newspaper."[185] Further, the Court stressed the burden placed on the newspaper, which, while not explicitly stated, suggested a failure of the "narrowly tailored" element of strict scrutiny: "a newspaper can[not] proceed to infinite expansion of its column space to accommodate the replies that a government agency determines or a statute commands the readers should have available."[186]

In *Wooley v. Maynard*,[187] the State of New Hampshire imposed criminal sanctions upon a Jehovah's Witness couple who covered up the portion of their license plate bearing the state's motto, "Live Free or Die," on the basis of religious objection to the text.[188] The Court concluded that the state was forcing the couple to "use their private property as a 'mobile billboard' . . . [and that] [t]he First Amendment protects the right of individuals . . . to refuse to foster, in the way New Hampshire commands, an idea they find morally objectionable."[189] The Court applied strict scrutiny, apparently assuming that the compelled speech at issue was content based.[190] The Court concluded that the state interest asserted—the ability to identify passenger vehicles—did not justify the law in question because the unique configuration of the letters on the plate already provided identification.[191] The forced display of a motto was too broad, and not narrowly tailored to this goal.[192]

### 2. Is Code Speech?

Before applying the content and scrutiny analysis, a court must determine whether the message at issue is "speech" in order to give it First Amendment coverage.[193] The question of whether something is speech is not always easy to

[181] *See, e.g.*, *Riley*, 487 U.S. at 795; *Wooley*, 430 U.S. at 714.

[182] *Miami Herald*, 418 U.S. at 243–44.

[183] *Id.* at 245.

[184] *Id.* at 256–58.

[185] *Id.* at 256 (emphasis added).

[186] *Id.* at 256–58.

[187] 430 U.S. 705 (1977).

[188] *Wooley*, 430 U.S. at 707–08.

[189] *Id.* at 715.

[190] *Id.* at 716.

[191] *Id.*

[192] *Id.* at 716–17.

[193] *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 570 (2011); Universal City Studios v. Corley, 273 F.3d 429, 446 (2d Cir. 2001).

answer, and no example illustrates that difficulty better than computer code.[194] Appellate courts that have addressed this question have all answered that code is speech.[195] However, there is sharp disagreement among scholars as to whether and when computer code qualifies for First Amendment protections.[196]

The debate can be traced to a fundamental difference in political and philosophical values.[197] Rooted in this difference is the wide variety of viewpoints concerning what exactly constitutes social expression.[198] Civil libertarians, for example, are more likely to support the notion that code is speech because they believe speech does not depend on mode or form.[199] They think speech is an end in itself.[200] Others, however, believe form is critical because speech is utilitarian in nature: it is a tool for communication, a means for sharing ideas that requires widespread understanding.[201]

The debate can generally be divided into three groups. The first group believes code is always speech, and cases that have decided this issue all support this position.[202] Those in the second group believe code is exclusively functional and is merely a device or machine, and thus can never be speech.[203] The third group argues that whether code is speech depends on the circumstances, such as the programmer's intent and the expressive value of the code.[204] This Section will summarize each of these arguments in turn.

#### *a. Viewpoint One: Code Is Always Speech*

*Bernstein v. United States Department of State*[205] was the first case to address the code-speech question, and it took a strong stance that code is always speech.[206] Daniel Bernstein, a Ph.D. candidate in mathematics, wanted to publish and share source code he had written as part of his graduate thesis.[207]

[194] Roig, *supra* note 26, at 322; *see also* E. John Park, *Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security*, VA. J.L. & TECH., Fall 1997, at art. 3, ¶¶ 1–4.

[195] David McGowan, *From Social Friction to Social Meaning: What Expressive Uses of Code Tell Us About Free Speech*, 64 OHIO ST. L.J. 1515, 1522 (2003).

[196] Roig, *supra* note 26, at 322–24.

[197] *See* McGowan, *supra* note 195, at 1539; Robert Plotkin, *Fighting Keywords: Translating the First Amendment to Protect Software Speech*, 2003 U. ILL. J.L. TECH. & POL'Y 329, 374.

[198] McGowan, *supra* note 195, at 1539.

[199] Plotkin, *supra* note 197, at 382.

[200] *See* Colangelo & Maurushat, *supra* note 38, at 50–51.

[201] *See id.* at 50.

[202] *See, e.g.*, Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 804 (2013). For an overview of these cases, see *infra* Part II.C.2.a.

[203] *See, e.g.*, Moerke, *supra* note 23, at 1027.

[204] *See, e.g.*, Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629, 654–55 (2000).

[205] 922 F. Supp. 1426 (N.D. Cal. 1996).

[206] *Bernstein*, 922 F. Supp. at 1436.

[207] *Id.* at 1428–30.

The code provided an encryption algorithm capable of protecting users' data.[208] The government determined that the code was a "defense article" under the International Traffic in Arms Regulations (ITAR) and the Arms Export Control Act (AECA), which meant that he needed a license to distribute the code.[209] The purpose of these regulations was to address the concern that new computer encryption technology could fall into the hands of dangerous foreign actors.[210] Bernstein argued that the code he had written was speech within the purview of the First Amendment.[211]

In its analysis of this then-novel argument, the Northern District of California concluded that computer source code is speech for purposes of the First Amendment.[212] It asserted that code is language, like French or German.[213] It also found irrelevant the idea that computer code is inherently functional because it directs a computer to complete a task.[214] It noted that this characteristic "does not make it any less like speech" just like "music inscribed in code on the roll of a player piano is no less protected for being wholly functional."[215]

The Sixth Circuit took a similar stance in *Junger v. Daley*.[216] Confronting the same regulations and similar facts as those in *Bernstein*, the court acknowledged that the issue of computer code is difficult because code has both an expressive and a functional purpose.[217] However, the court asserted that code's functional capacity should not, on its own, undermine constitutional protection.[218] Like *Bernstein*, *Junger* analogized code to music and painting, stating that while untraditional, computer code is an expressive means of exchanging information about computer programming itself.[219] That is, computer programmers can communicate to each other through computer code, which reinforces its classification as speech.[220]

The Southern District of New York in *Universal City Studios, Inc. v. Reimerdes*[221] mirrored the reasoning in *Junger* and *Bernstein*, although it approached the issue in a different context.[222] A programmer created software

[208] *Id.* at 1429.

[209] *Id.* at 1430.

[210] Fox, *supra* note 30, at 886–87.

[211] *Bernstein*, 922 F. Supp. at 1434.

[212] *Id.* at 1436.

[213] *Id.* at 1435.

[214] *Id.*

[215] *Id.*

[216] 209 F.3d 481 (6th Cir. 2000).

[217] *Junger*, 209 F.3d at 484.

[218] *Id.*

[219] *Id.*

[220] *See id.*

[221] 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[222] *See Reimerdes*, 111 F. Supp. 2d at 304.

that could decrypt DVDs and allow a user to copy their content.[223] Movie studios sued him under the Digital Millennium Copyright Act (DMCA),[224] a federal statute that makes it illegal to publish certain technologies that were developed to defeat technological protections against unauthorized access to a work.[225] The court found that code is expressive,[226] stating that "[i]t cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine."[227] While not everyone understands code, according to the court, not everyone understands English, either.[228] Each language conveys ideas, though in different ways.[229] Thus computer code, like movies, books, and art, is covered by the First Amendment.[230]

On appeal, the Second Circuit agreed with the decision in *Universal City Studios, Inc. v. Corley*.[231] The court reasoned that while the Framers may not have been thinking of computer code, they also were not thinking about radio or movies, yet each of those receives First Amendment coverage.[232] Further, the court equated computer code to math formulas, stating that "symbolic notations not comprehensible to the uninitiated" still should be afforded First Amendment protection.[233] Lastly, the court analogized code to a cooking recipe: recipes are not exempted from coverage because they require the use of an oven, and code should not be exempted because it requires a computer.[234]

For the most part, academic arguments in absolute support of code as speech parallel those arguments presented in the court decisions above. Some assert that code is expressive in its instructional value.[235] Others emphasize the First Amendment interest in the free flow of scientific information.[236]

#### b. *Viewpoint Two: Code Is Never Speech*

In a contrasting view, critics of computer code as speech typically point to code's functionality and purpose. That is, unlike a bumper sticker, code is not written to make a statement;[237] code is the implementation of an idea rather than

[223] *Id.* at 303.

[224] *Id.*

[225] *Id.* at 316.

[226] *Id.* at 304.

[227] *Id.* at 326.

[228] *Id.*

[229] *Id.*

[230] *Id.* at 327.

[231] 273 F.3d 429, 435 (2d Cir. 2001).

[232] *Corley*, 273 F.3d at 434.

[233] *Id.* at 445.

[234] *Id.* at 447; *see also* 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1099 (N.D. Cal. 2004) (holding that code is speech without analysis of the issue); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002) (same).

[235] *See, e.g.*, Halpern, *supra* note 276, at 182.

[236] *See, e.g.*, Park, *supra* note 194, ¶ 51.

[237] Moerke, *supra* note 23, at 1029.

the idea itself.[238] Thus, code simply acts as a machine or a tool that carries out an intended function.[239] In this way it is similar to a pen or a paper, which facilitate the expression of an idea rather than symbolize the idea itself.[240] In response to the argument that code is like protected music, critics argue that code is not the music—it is the motors, levers, gears, and wires that all work together to create the music, and these are not protected.[241]

### *c. Viewpoint Three: Whether Code Is Speech Depends on the Circumstances*

While some take the hard stances—that code is always or never speech—a well-developed viewpoint in scholarship is that code can be, but is not necessarily, speech. As one scholar has noted, the question of whether software is speech is the wrong one.[242] The proper inquiry is not whether something is inherently speech but whether the speaker intended to speak.[243] Of course, this viewpoint runs in stark contrast to the libertarian view that speech is an end in itself, and therefore the "why" is irrelevant.[244] However, scholars in this third group believe the intent of the programmer should drive the analysis,[245] as well as the "social circumstances of [code's] sale and application."[246] If the purpose of code is solely to communicate to a computer, this code could be deserving of less protection.[247] Code that is written on a t-shirt, for example, would likely be speech because it is not written to communicate to a machine but rather to the public.[248] Similarly, code that is created to encourage discussion could be speech as well.[249]

These writers also assert that the debate over whether software is expressive or functional is a false dichotomy.[250] Architecture, for example, is both, and it can be protected speech.[251] Further, the fact that many do not understand computer code is irrelevant, for relatively few understand Braille, yet that language is obviously protected.[252] Those in this third group also take a nuanced

[238] *Id.* at 1043.

[239] Ocrant, *supra* note 23, at 539.

[240] *Id.*

[241] *Id.* at 540.

[242] Tien, *supra* note 204, at 634.

[243] *Id.*

[244] *See* Plotkin, *supra* note 197, at 382.

[245] Tien, *supra* note 204, at 634; *see also* Matwyshyn, *supra* note 202, at 798–99.

[246] Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 720 (2000).

[247] *See id.* at 720–21; *see also* Bonnie L. Schriefer, Comment, *"Yelling Fire" and Hacking: Why the First Amendment Does Not Permit Distributing DVD Decryption Technology*, 71 FORDHAM L. REV. 2283, 2324 (2003).

[248] Matwyshyn, *supra* note 202, at 807.

[249] Schriefer, *supra* note 247, at 2324.

[250] Plotkin, *supra* note 197, at 337–38.

[251] *Id.*

[252] Tien, *supra* note 204, at 677.

view toward the case law. Some argue that cases like *Junger* focus too much on the fact that code simply looks like a language and ignore other factors.[253] The code in *Bernstein*, for example, was not written to communicate to a computer; rather, it was posted on a website to teach others how to write code.[254] Thus, the communication aspect is important, and this group asserts that cases like *Bernstein* should not be read too broadly to encompass all code everywhere.[255]

### *D. The Doctrine of Constitutional Avoidance*

There are a variety of ways that a future court could apply this vast body of law to the issue of law enforcement compelling technology companies to write computer code. A court may, for example, conclude that code is not speech and hold that the First Amendment does not apply. It would then look to the All Writs Act to determine whether it permits the type of compulsion the FBI sought following San Bernardino.

A court might also apply the doctrine of constitutional avoidance and not reach the First Amendment matter.[256] This doctrine is actually a substantive canon of statutory interpretation in which a court will, if possible, reasonably interpret a statute in such a way that avoids addressing a constitutional issue.[257] The Court in *United States ex rel. Attorney General v. Delaware & Hudson Co.*[258] articulated the doctrine as follows: "where a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, our duty is to adopt the latter."[259]

There are numerous justifications for this doctrine. First, a federal court will only address a constitutional question when absolutely necessary.[260] Further,

[253] *See, e.g.*, Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1292–93 (2000).

[254] Patrick Ian Ross, Recent Case, Bernstein v. United States Department of State, 13 BERKELEY TECH. L.J. 405, 415 (1998).

[255] *Id.*

[256] *See, e.g.*, Richard L. Hasen, *Constitutional Avoidance and Anti-Avoidance by the Roberts Court*, 2009 SUP. CT. REV. 181, 189. *But see* Hedberg, *supra* note 22, at 697 (asserting that avoidance doctrine can be a form of judicial activism rather than judicial restraint).

[257] *See* Hasen, *supra* note 256, at 189. In *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 (1936), Justice Brandeis articulated what is now considered the modern avoidance canon. *Id.* at 347 (Brandeis, J., concurring); *see also* T.J. Fosko, Note, *Avoiding the Unavoidable: The Canon of Constitutional Avoidance as Applied to the Patient Protection and Affordable Care Act*, 35 U. ARK. LITTLE ROCK L. REV. 591, 594 (2013). In applying the modern canon, courts will refuse even to answer the constitutional question unless there is no other way to adjudicate a case. Fosko, *supra*, at 596; *see, e.g.*, Nw. Austin Mun. Util. Dist. No. One v. Holder, 557 U.S. 193, 197 (2009) [hereinafter *NAMUDNO*] ("[This] constitutional question has attracted ardent briefs from dozens of interested parties, but the importance of the question does not justify our rushing to decide it.").

[258] 213 U.S. 366 (1909).

[259] *Del. & Hudson Co.*, 213 U.S. at 408.

[260] *See NAMUDNO*, 557 U.S. at 197 ("Our usual practice is to avoid the unnecessary resolution of constitutional questions."). Chief Justice Roberts's opinion in *National Federation of Independent Business v. Sebelius*, 567 U.S. 519 (2012), in which he overtly evaluated the

federal courts want to show respect for the principle of the separation of powers by avoiding the invalidation of statutes on constitutional grounds.[261] This is especially true when a statute is ambiguous and thus legislative intent is unclear.[262] In this circumstance, courts are willing presume that Congress did not intend to violate the Constitution.[263]

To reach the doctrine of constitutional avoidance, a court must first determine that there is a serious constitutional problem that must be avoided.[264] One writer described it as follows: "the avoidance canon first requires judges to engage in a preliminary factual inquiry to determine whether a litigant's claim poses a risk of requiring constitutional adjudication at all."[265] The threshold level of risk that warrants avoidance is unclear in case law, as some judges have been more willing than others to defer an issue to the legislature.[266]

Once a court determines that a constitutional issue exists, the court will then

constitutionality of each potential interpretation, is in fact an exception to this rule. Eric S. Fish, *Constitutional Avoidance as Interpretation and as Remedy*, 114 MICH. L. REV. 1275, 1284 (2016).

[261] *See* Lisa A. Kloppenberg, *Avoiding Serious Constitutional Doubts: The Supreme Court's Construction of Statutes Raising Free Speech Concerns*, 30 U.C. DAVIS L. REV. 1, 3 (1996); Michael L. Wells, *The "Order-of-Battle" in Constitutional Litigation*, 60 SMU L. REV. 1539, 1548 (2007) (explaining that the goal is to "minimize the friction" between the legislature and the judiciary). A court will try to construe a statute fairly to avoid constitutional problems unless this construction is plainly contrary to Congress's intent. Fosko, *supra* note 257, at 596; *see also Sebelius*, 567 U.S. at 537–38 (explaining that the court has a "general reticence to invalidate the acts of the Nation's elected leaders" unless unconstitutionality is "clearly demonstrated" (quoting United States v. Harris, 106 U.S. 629, 635 (1883))).

[262] Fish, *supra* note 260, at 1289 (noting Judge Guido Calabresi's viewpoint that constitutional avoidance is a means of "interbranch dialogue").

[263] *See* Charlotte Garden, *Religious Employers and Labor Law: Bargaining in Good Faith?*, 96 B.U. L. REV. 109, 130–31 (2016). *But see* Hasen, *supra* note 256, at 190 (explaining that for the Warren Court, statutory ambiguity was not a necessary condition to constitutional avoidance, so long as it determined that Congress had not actively considered an issue).

[264] *See* Fosko, *supra* note 257, at 596. The modern avoidance canon has a lower standard for finding a potential constitutional problem than the classical avoidance canon. Fish, *supra* note 260, at 1282. Unlike the classical canon, the modern canon generally requires only a "good chance" of a constitutional issue, or a constitutional doubt—not necessarily an actual issue. *Id.* This is the prevailing approach. *Id.* at 1284.

[265] Anthony Vitarelli, Comment, *Constitutional Avoidance Step Zero*, 119 YALE L.J. 837, 837 (2010). Courts' refusal to openly conduct this inquiry has subjected the doctrine to some criticism. *See, e.g.*, *id.* at 842 ("Courts should openly acknowledge [this preliminary] inquiry and should enunciate an explicit standard for future cases."); Justin Collings, *Appealing to Congress*, 50 U.C. DAVIS L. REV. 463, 467 (2016) (arguing that courts should more openly assert the presence of constitutional issues so the legislature may address them).

[266] *See* Vitarelli, *supra* note 265, at 841–42. Justice O'Connor, for example, was more willing to apply avoidance—her standard was whether there was mere potential to "upset the usual constitutional balance of federal and state powers." *Id.* at 840 (quoting Gregory v. Ashcroft, 501 U.S. 452, 460 (1991)). Justice Scalia was relatively unwilling to avoid a constitutional issue and wanted to apply the doctrine as a kind of last resort. *See* Fish, *supra* note 260, at 1286; Garden, *supra* note 263, at 132–33. He had a high standard for application: he would avoid adjudicating a constitutional issue *only* if the issue "push[ed] the outer limits" of constitutional law. Vitarelli, *supra* note 265, at 842. (quoting Gonzales v. Oregon, 546 U.S. 243, 291 (2006) (Scalia, J., dissenting)).

move to evaluate the statute itself.[267] As an illustration, in *Northwest Austin Municipal Utility District Number One v. Holder (NAMUDNO)*,[268] a small municipal utility district sought relief from preclearance requirements under Section 5 of the Voting Rights Act (VRA), which forbade any changes to state election procedures unless approved by a court.[269] Under the VRA, a "State or political subdivision" could be "bail[ed] out" of this requirement if there have been no voting rights issues in the district for ten years.[270] The utility district sought the bailout, which was denied because a court determined that it did not qualify as a "State or political subdivision" because it did not register voters.[271] As a result, the utility district questioned the constitutionality of the VRA.[272] The Supreme Court called this a "big question."[273] But the Court never reached the question, instead finding statutory justification to define the utility district as a "political subdivision" eligible for bailout.[274] In so doing, it avoided the constitutional question entirely.[275]

## III. Discussion

The San Bernardino battle is over, but the technological war rages on. A similar confrontation will occur over the All Writs Act. And, once more, the First Amendment will be placed in the spotlight. Due to the rise of encryption and its growing adoption by technology companies,[276] law enforcement will necessarily need to circumvent encryption or access data through a backdoor. Since the technology industry is reaching a point where even certain technology companies cannot access their consumers' data,[277] the government will be forced to compel companies to write code to allow for data access, thus triggering First Amendment concerns.[278]

Take, for example, Apple itself. Apple had previously helped law

[267] *See, e.g.*, *NAMUDNO*, 557 U.S. 193, 198 (2009).

[268] 557 U.S. 193 (2009).

[269] *NAMUDNO*, 557 U.S. at 196–97.

[270] *Id.* at 199, 201.

[271] *Id.* at 201.

[272] *Id.* at 197.

[273] *Id.* at 196.

[274] *Id.* at 208–11.

[275] *Id.* at 211. *NAMUDNO* has been criticized for its implausible statutory interpretation. *See* Neal Kumar Katyal & Thomas P. Schmidt, *Active Avoidance: The Modern Supreme Court and Legal Change*, 128 HARV. L. REV. 2109, 2112–13 (2015). Justice Scalia was often concerned that to avoid a potential constitutional problem, the Court was effectively rewriting statutes. Garden, *supra* note 263, at 132–33; *see also* Fish, *supra* note 260, at 1275 (noting the history of rather extreme statutory readings). A Scalia-like approach would employ avoidance as a tiebreaker in the presence of two competing statutory interpretations, each of which is equally plausible. Hasen, *supra* note 256, at 186.

[276] *See* Miller, *Google and Apple*, *supra* note 41.

[277] *See* Lee, *Apple's Battle Explained*, *supra* note 42.

[278] See *supra* Part II.B.2.b for a discussion of the most recent attempts to do this under the All Writs Act.

enforcement access iPhones before it had implemented default encryption.[279] Apple simply withdrew users' nonencrypted data from iPhones and handed it over to authorities.[280] But this method of assistance is nearing irrelevance. Apple and other companies are strengthening their encryption, meaning that without an encryption key, any data Apple produces will be unintelligible.[281] The FBI cannot ask Apple to unscramble a user's phone data because Apple does not store individual encryption keys.[282] Any attempt to open the phone by guessing the relevant passcode could be thwarted by an iPhone security feature that wipes the data clean after ten failed guesses.[283] Thus, for law enforcement to access data, it must force Apple to write code to remove certain security features from the phone—as the FBI tried to do after San Bernardino.[284]

Since the technological future of data access lies in forced code writing, the legal future lies in First Amendment doctrine. In resolving future cases involving compelled code writing, a court should apply the canon of constitutional avoidance, which will evade a First Amendment adjudication in rejecting the government's authority to compel code writing under the All Writs Act. Part III.A of this Section will explain the reasons for avoiding judicial entanglement: the All Writs Act is highly ambiguous, its legislative intent is unclear, and the issues involved are politically charged such that the legislative branch is better suited to resolve them.

Part III.B will demonstrate that a legitimate First Amendment issue exists, which is the first step in a constitutional avoidance analysis.[285] Specifically, the code-is-speech argument is strong, as is the argument concerning what level of judicial scrutiny a court should apply. Since the First Amendment issues here are apparent, a court should avoid them and move to the All Writs Act to determine if an exclusively statutory interpretation in favor of Apple is available. Part III.C will show that such an interpretation is available—the All Writs Act can readily be interpreted in a way that does not grant the government the authority it seeks. This conclusion avoids the difficult First Amendment question, results in a victory for Apple, and defers the issue to Congress. Part III.D will assert that Congress must create a new statutory regime to replace the All Writs Act.

### A. *Justifications for Avoidance*

There are numerous justifications a court may use to apply the avoidance doctrine when confronting a constitutional question that has the potential to upend a statute. Three are particularly relevant in this context:

[279] *See* Smythe, *supra* note 72.

[280] *See id.*

[281] *See* Yadron, *supra* note 21.

[282] *See* Lee, *Apple's Battle Explained*, *supra* note 42.

[283] *See id.*; Lee, *Upgrade Your iPhone*, *supra* note 50.

[284] *See* Government's Motion to Compel, *supra* note 13, at 2.

[285] *See* Fosko, *supra* note 257, at 596.

statutory ambiguity,[286] uncertain legislative intent,[287] and deference to Congress on sensitive political issues.[288]

Statutory ambiguity is an important factor in the decision to avoid a constitutional issue.[289] This gets to one presumption underlying the avoidance doctrine: that the legislature, in passing a statute, never envisioned its drafting to be unconstitutional.[290] Therefore, it would be inappropriate to invalidate a statute on constitutional grounds if that statute could plausibly be read to meet constitutional scrutiny.[291] Where language is unclear, furthermore, a court likely cannot accurately access a statute's scope. For this reason, it would hesitate to essentially condemn a legislature's action when it cannot glean from the statutory text the true meaning of the legislative act.[292]

The All Writs Act is as ambiguous as statutes come. Beyond facially confusing language, case law interpreting it has confirmed its vagueness. Before 1977, courts varied widely in their interpretation and application of the Act[293]—some courts openly acknowledged this.[294] In 1977, *New York Telephone* provided a framework.[295] But that framework comprised a set of discretionary factors extrinsic to the statutory text.[296] And, even with the *New York Telephone* framework, courts still have varied widely in their interpretation of the All Writs Act.[297]

Relatedly, the legislature's intent in enacting the All Writs Act is unclear. Legislative intent is a factor to which courts turn when applying the avoidance doctrine.[298] The justification for this is similar to the reasoning behind statutory ambiguity as a factor: where a court is unable to divine what the legislature was thinking, it would be unfair to presume that it intended to pass an unconstitutional statute.[299] The Court in *New York Telephone* did not even attempt to analyze the legislature's intent in enacting the Act.[300] Furthermore, the general purpose of the All Writs Act was to be a gap-filler in requiring

[286] Fish, *supra* note 260, at 1289 (discussing Judge Guido Calabresi's belief that statutory ambiguity is a relevant justification for constitutional avoidance).

[287] *Id.*; Hedberg, *supra* note 22, at 681.

[288] Political controversy surrounding a constitutional challenge is a recognized justification for avoidance. *See* Hasen, *supra* note 256, at 183.

[289] Fish, *supra* note 260, at 1289.

[290] Garden, *supra* note 263, at 130–31.

[291] *Id.*

[292] *See id.*

[293] See *supra* Part II.B.1 for a review of these decisions.

[294] *See, e.g.*, Klay v. United Healthgroup, Inc., 376 F.3d 1092, 1102 (11th Cir. 2004).

[295] United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977).

[296] *See id.*

[297] See *supra* Part II.B.2 for a discussion of the varying applications following *New York Telephone*.

[298] *See* Hedberg, *supra* note 22, at 681.

[299] *See id.* at 681–82.

[300] 434 U.S. at 172–78.

parties to assist in criminal investigations.[301] It would be hard to imagine that the 1789 legislature could have expected that one day such assistance would raise First Amendment questions.

Separation of powers is another justification for avoidance.[302] Avoiding constitutional invalidation by focusing on a statutory reading would, in effect, "punt" the question to the legislature, which could amend the statute or create a completely new one.[303] A court exposes itself to charges of improperly legislating political problems from the bench when it reads a statute so as to avoid a ruling on its constitutionality where such a reading exists.[304] Courts are often concerned that this image undermines their legitimacy.[305] Thus, avoidance can be a kind of "overture" to the legislature.[306]

This Comment does not purport to delve into the complex issue of political questions and federal jurisdiction; it only reminds that the presence of big-picture policy ramifications is a recognized justification for the avoidance doctrine.[307] The controversy following San Bernardino illustrates that Congress is the more appropriate venue for resolving these questions. First, it actually attempted to resolve them.[308] A few months after the attack, Senators Burr and Feinstein drafted a bill to clarify the encryption issue.[309] Second, the FBI's attempt to force Apple to write code exploded into a nationwide debate.[310] It generated a variety of policy questions, including the proper role for law enforcement, the importance of data security, the scope of free speech, the growing concern over terrorism, and the need for effective criminal justice.[311]

[301] See *supra* Part II.B for an explanation of the mechanics of the All Writs Act.

[302] *See* Wells, *supra* note 261, at 1547–48.

[303] *See* Collings, *supra* note 265, at 467. Some are skeptical of Congress's ability and willingness to respond. *See, e.g.*, Fish, *supra* note 260, at 1291 ("[T]he high degree of legislative inertia in the American political system undermines the . . . assertion that avoidance is simply a matter of giving the legislature a 'second look.'"); Garden, *supra* note 263, at 135–36 ("[A]mending a statute to address [a court's narrowing of it] will probably require a new set of legislative compromises; when the underlying legislation is controversial, proponents could reasonably fear that reopening the issue to override a court decision will risk losing more than could be gained.").

[304] *See* Katyal & Schmidt, *supra* note 275, at 2127.

[305] *See id.*

[306] Garden, *supra* note 263, at 129–30; *see also* Fish, *supra* note 260, at 1288 ("The classical argument for the avoidance canon is that it is more democratic to send legislation back to Congress than to strike it down.").

[307] *See* Hasen, *supra* note 256, at 183–84.

[308] *See* Compliance with Court Orders Act of 2016, S.___, 114th Cong. (discussion draft as proposed by S. Comm. on Intelligence, Apr. 13, 2016), http://feinstein.senate.gov/public/index.cfm?a=files.serve&File_id=5B990532-CC7F-427F-9942-559E73EB8BFB [perma: http://perma.cc/K8V7-SWY8]; *see also* Press Release, Office of Senator Dianne Feinstein, Intelligence Committee Leaders Release Discussion Draft of Encryption Bill (Apr. 13, 2016) (available at http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649 [perma: http://perma.cc/Q39X-RNE8]). The draft, however, never made it past discussion.

[309] *See supra* note 308.

[310] *See, e.g.*, Orlando, *supra* note 17.

[311] See *supra* Part I.A for a background of this case and the policy questions it generated.

Third, both Apple and the FBI argued that this issue should ultimately be decided by Congress—not the courts.[312]

For these reasons, if a court is confronted with the forced encryption issue, it should apply constitutional avoidance. The All Writs Act is ambiguous, the legislative intent behind it is unclear, and the political controversy surrounding forced code writing is significant. The separation of powers doctrine—always a concern for courts and an underlying justification for avoidance[313]—touches on each of these factors. Thus, avoidance offers a "way out" for federal judges concerned about judicial overreach into the legislative realm.

Beyond these judicially recognized reasons to apply the constitutional avoidance doctrine, there is one simpler still. Forced code writing based on the All Writs Act is not susceptible to the common criticisms of the avoidance doctrine.[314] These criticisms vary, but two are most prominent.[315] First, critics assert that many judges are too eager to find a constitutional issue when one is not actually there.[316] The reason is simple: if a judge can find a constitutional issue, he can read a statute to avoid the issue and is thus not required to strike down the statute.[317] The First Amendment analysis below will show that the constitutional argument here is strong and involves none of the "theorizing" that critics suggest is prevalent in avoidance application.[318]

A second common criticism is that judges go to extreme lengths in reading statutes to avoid constitutional issues to the point that they are effectively rewriting them.[319] Again, the motivation is an unwillingness to invalidate legislative action on constitutional grounds.[320] The All Writs analysis below will

[312] Geoff Dyer, *Apple and FBI in Plea for Encryption Legislation*, FIN. TIMES (Mar. 1, 2016), http://www.ft.com/content/994168ce-df3b-11e5-b072-006d8d362ba3 [perma: http://perma.cc/GFK7-WE7P].

[313] *See* Wells, *supra* note 261, at 1548.

[314] *See, e.g.*, Katyal & Schmidt, *supra* note 275, at 2111–12 (arguing that the modern use of the avoidance doctrine "now camouflages acts of judicial aggression in both the constitutional and statutory spheres").

[315] *Id.*

[316] *Id.* ("[A]voidance leads to . . . sloppy and cursory constitutional reasoning. . . . The avoidance canon requires only that a judge advert to some theoretical 'doubt' about a law's constitutionality, which naturally leads to vague and imprecise constitutional analysis.").

[317] *See* Fish, *supra* note 260, at 1290–91 ("[B]ecause judges are not forced to actually strike down a law in the case at bar, they are more willing to go out on a limb in their constitutional theorizing and announce new constitutional doctrines.").

[318] *See id.* See also *infra* Part III.B for a discussion of the analysis a court will conduct concerning the First Amendment issue in compelled code cases.

[319] This has been called, among other things, "[a]voiding the [u]navoidable," Fosko, *supra* note 257, at 591, and "[a]ggressive constitutional avoidance," Garden, *supra* note 263, at 112.

[320] *See* Fish, *supra* note 2601, at 1290–91. Justice Scalia was among these critics. *See* Garden, *supra* note 263, at 132–33. He argued that an alternative statutory interpretation must be plausible; otherwise, the doctrine would be unpredictable and arbitrary. *See* Hasen, *supra* note 256, at 186, 189–90. Chief Justice Roberts's opinions in *NAMUDNO*; *Sebelius*; and *Shelby County v. Holder*, 133 S. Ct. 2612 (2013), are often criticized for this reason. *See* Katyal & Schmidt, *supra* note 275, at 2110–12. One writer described Roberts's approach to statutory interpretation as resulting in "an opinion for eight justices that adopted a strained reading of Section 5 of the Voting Rights Act to avoid confronting the

demonstrate that statutory interpretation in this case is plausible to say the least. Thus, the common criticisms of avoidance application are invalid here.

### *B. The First Amendment Issue*

The first step of the avoidance doctrine requires the court to identify a serious constitutional issue.[321] However, it is not clear how grave the question must be—as discussed above,[322] Justices have different standards.[323] Further, it is not clear from the avoidance cases the extent to which the court actually analyzed the constitutional issue outside of identifying it in the written opinion.[324] A federal court will not officially adjudicate the constitutional question unless it is necessary.[325] For example, in *NAMUDNO*, the Court identified a "big question" of constitutional law and then ignored it entirely and focused exclusively on statutory interpretation.[326] We are left to assume that the Court engaged in some sort of analysis to determine that there was in fact a constitutional issue to begin with.

This Part will discuss the inquiry a court will conduct ex ante regarding the First Amendment problem for compelled code. This inquiry is divided into two questions that a court will ask to determine whether a legitimate First Amendment problem exists: the coverage question and the scrutiny question.[327] These questions will persuade a court that there exists a serious First Amendment basis for invalidating the All Writs Act. What is more, this Part will demonstrate that even the highest standard for avoidance—a Scalia-like requirement that the potential issue "push the outer limits of constitutional protection"[328]—is satisfied here.

#### 1. The Coverage Question

Whether code is covered by the First Amendment is a challenging—and hotly debated—issue.[329] On the one hand, case law addressing computer code can be distinguished from the FBI's order to Apple because the order required

question of its constitutionality." Jonathan H. Adler, *Chief Justice John Roberts and Constitutional Avoidance*, VOLOKH CONSPIRACY (July 12, 2012, 8:28 PM), http://volokh.com/2012/07/12/chief-justice-roberts-and-constitutional-avoidance [perma: http://perma.cc/6MFH-UHKE] (citing Rick Hasen, *Was Chief Justice Roberts Most Unprincipled in Applying the Doctrine of Constitutional Avoidance in the Health Care Case, in* NAMUDNO *(the Voting Rights Act Case) or in* Citizens United*?*, ELECTION L. BLOG (July 11, 2012, 9:57 PM), http://electionlawblog.org/?p=36823 [perma: http://perma.cc/TX4L-KQHK]).

[321] *See* United States *ex rel.* Attorney Gen. v. Del. & Hudson Co., 213 U.S. 366, 408 (1909).

[322] See *supra* Part II.D for a discussion of the constitutional avoidance doctrine.

[323] *See* Vitarelli, *supra* note 265, at 841.

[324] *See id*. at 842.

[325] *See, e.g.*, *NAMUDNO*, 557 U.S. 193, 197 (2009).

[326] *Id.* at 196–97.

[327] *See* Vitarelli, *supra* note 265, at 838.

[328] *Id.* at 842 (quoting Gonzales v. Oregon, 546 U.S. 243, 291 (2006) (Scalia, J., dissenting)).

[329] See *supra* notes 197–255 and accompanying text for a discussion of the competing viewpoints.

Apple to write encryption code applicable only to the suspect's iPhone.[330] In *Bernstein*, for example, the PhD candidate who wrote the code wanted to share it with the world.[331] While the code ultimately may have been inputted into a machine, Bernstein sought to publish it so that others could evaluate it.[332] Similarly, in *Reimerdes*, the plaintiff published the decryption code on his website, a public forum.[333] Even in *United States v. Elcom Ltd.*,[334] in which the plaintiff company sought to sell code rather than openly publish it, the code would have reached someone other than the company itself.[335] Apple's encryption software, on the other hand, would have been written by Apple and uploaded into the suspect's phone without anyone else laying eyes on the code.[336]

While *Bernstein*, *Reimerdes*, and *Elcom* can be distinguished from forced decryption, each strongly asserts that code is speech regardless of surrounding circumstances.[337] In *Bernstein*, for example, the court found that code's functionality was irrelevant in the coverage determination.[338] In plain words it stated that "source code is speech."[339] The court in *Junger* likewise found functionality to be a nonissue in the coverage question.[340] And the *Reimerdes* court mirrored the *Bernstein* court's directness: "It cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine."[341] Thus, these courts assert that, whether or not code is intended to be viewed by the public (as it was in those cases), it must, at a minimum, implicate some First Amendment coverage.

Beyond prior case law, a court should also be persuaded by code's similarity to math, music, or art. Each of these methods of expression is written in code form. Computer code may be untraditional, but its uniqueness should not preclude its protection under the First Amendment.[342] The purpose of elevator music may be to provide a comfortable atmosphere in an otherwise cramped space. The purpose of music in a football game may be to announce the entrance of the home team. If code's functionality meant no First Amendment coverage, then the government would be able to regulate those types of music without any remote concern about free speech rights.

[330] *See* Government's Motion to Compel, *supra* note 13, at 2.

[331] *See* Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1430 (N.D. Cal. 1996).

[332] *Id.*

[333] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 303 (S.D.N.Y 2000), *aff'd sub nom.* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[334] 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

[335] *See Elcom*, 203 F. Supp. 2d at 1118.

[336] *See* Government's Motion to Compel, *supra* note 13, at 14–15.

[337] *See infra* notes 341–44 and accompanying text.

[338] Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

[339] *Id.* at 1436.

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

[341] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 326 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[342] *See Junger*, 209 F.3d at 484–85 (noting that music is functional as well).

A court engaging in this coverage inquiry should find that a First Amendment issue exists, meaning that there will likely be a "big question" of constitutional law that a court will seek to avoid if possible.[343] The potential scrutiny analysis that a court may consider should it determine that code is speech enhances this question. While it is unclear whether a scrutiny consideration would be a part of a court's preliminary First Amendment avoidance inquiry, this next Part will nevertheless analyze it, as it exacerbates the First Amendment issue.

### 2. The Scrutiny Question

If a court rightly decides that code writing is *covered* by the First Amendment, then it must next consider a scrutiny analysis to determine whether code writing *violates* the First Amendment. Again, it is unclear how significant a factor this analysis would be in an ex ante avoidance inquiry.[344] Given that the scrutiny question might be more complicated than the coverage question, however, it will likely be significant in the decision to avoid the First Amendment issue entirely. The first component of the scrutiny question is straightforward: compelled decryption code is almost certainly a content-neutral government action because decryption code is inherently less expressive than other forms of code. The second component of the scrutiny question, the application of intermediate scrutiny, is decidedly more complex.

#### *a. Content Neutrality*

Apple argued that the government's compulsion was content based because it targeted Apple for its ideological viewpoint on privacy and data protection.[345] If so, Apple's encryption code would receive the same protection as the speech in *Miami Herald* (political candidates' speech) and *Wooley* ("Live Free or Die")—both content-based examples.[346] This is illogical. Apple's code is distinct from *Miami Herald* and *Wooley* in which there were clear ideological and even political components to the speech involved.[347] Apple's encryption code, on the other hand, is more tangentially symbolic of certain views rather than expressive of those views. Further, the decryption code the FBI requested is necessarily instructive and designed to be communicated solely to a machine. In *Miami Herald* and *Wooley*, by contrast, the speech was highly expressive and targeted at human audiences.[348] As one court noted, subjecting all computer code to strict scrutiny would "turn centuries of our law and legal tradition on its head, eviscerating the carefully crafted balance between protecting free speech and

[343] *See NAMUDNO*, 557 U.S. 193, 196 (2009).

[344] *See* Vitarelli, *supra* note 265, at 841.

[345] *See* Apple's Brief, *supra* note 17, at 33.

[346] Wooley v. Maynard, 430 U.S. 705, 707–08 (1977) (license plate slogan); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 243–44 (1974) (political candidates' speech); *accord* Frudden v. Pilling, 742 F.3d 1199, 1201 (9th Cir. 2014) (compelled school uniforms).

[347] *See Wooley*, 430 U.S. at 707–08; *Miami Herald*, 418 U.S. at 243–44.

[348] *See Wooley*, 430 U.S. at 707; *Miami Herald*, 418 U.S. at 234–44.

permissible governmental regulation."[349]

Importantly, all cases dealing with the regulation of encryption code have proclaimed that the regulations were content neutral.[350] While none of those cases were examples of compelled speech, the law generally treats compelled speech and prohibited speech similarly.[351] The principle inquiry regarding content neutrality is whether the government action was adopted because of agreement or disagreement with the substantive views of the message.[352]

In the Digital Millennium Copyright Act (DMCA) cases, for example, courts found that the reason the government enacted the statute had nothing to do with particular ideas.[353] The *Reimerdes* court made the following analogy: laws prohibiting the possession of burglar tools are not passed because of disagreement with a burglar's desire to express himself by possessing them.[354] In other words, regulation can divorce the expressive and functional components of speech.[355] The *Corley* court explained that decryption regulations were not concerned with the code's capacity to communicate with others; rather, they focused on the code's functional capability.[356] The court in *Elcom*, too, found that antitrafficking measures were enacted due to the functional capability of code.[357] Similarly, the FBI's order to Apple was requested not because the FBI disagreed ideologically with Apple's views on privacy. While Apple's decryption code may have, in fact, communicated ideas to programmers,[358] the FBI's order was "justified without reference to the [substantive] content of" any such speech.[359]Law enforcement needed access to an iPhone to aid a criminal investigation.[360]

On the other hand, the FBI is arguably targeting technology companies based on their viewpoints because the FBI would only issue requests to those companies that, like Apple, employ encryption by default—perhaps a signal of the companies' views on privacy. That argument, however, is weak and has already been addressed and rejected. In *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*,[361] for example, the plaintiffs argued that the DMCA was

[349] United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1128 (N.D. Cal. 2002).

[350] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 454–56 (2d Cir. 2001); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1100 (N.D. Cal. 2004); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 329 (S.D.N.Y. 2000), *aff'd sub nom. Corley*, 273 F.3d 429.

[351] Riley v. Nat'l Fed'n of the Blind of N.C., 487 U.S. 781, 797 (1988).

[352] Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989); *Elcom*, 203 F. Supp. 2d at 1128; *Reimerdes*, 111 F. Supp. 2d at 329.

[353] *See, e.g.*, *Reimerdes*, 111 F. Supp. 2d at 329.

[354] *Id.*

[355] *Elcom*, 203 F. Supp. 2d. at 1128–29.

[356] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 454 (2d Cir. 2001).

[357] *Elcom*, 203 F. Supp. 2d at 1128.

[358] *See* Plotkin, *supra* note 197, at 330.

[359] *See Corley*, 273 F.3d at 450 (quoting Hill v. Colorado, 530 U.S. 703, 720 (2000)).

[360] Government's Motion to Compel, *supra* note 13, at 2.

[361] 307 F. Supp. 2d 1085 (N.D. Cal. 2004).

impermissible viewpoint discrimination because it banned only encryption-circumvention technology.[362] The *321 Studios* court responded that the statute bans only the functional element of the code rather than the speech in the code because of its content.[363] The *Reimerdes* court similarly held that while circumvention was targeted to some extent, this was the function of code rather than its expressive feature and thus was content neutral.[364] It analogized to *City of Renton v. Playtime Theaters, Inc.*,[365] in which adult movie theaters were banned from a neighborhood.[366] The *City of Renton* court found the regulation was not passed due to the government's ideological disagreement with the content of the films.[367] Rather, the concern was the secondary effects that showing the films would have on the neighborhood.[368] For this reason, the regulation was content neutral.[369] Similarly, the FBI was not concerned with Apple's stance on privacy but the secondary effects that its encryption technology would have on the San Bernardino criminal investigation.[370] Thus, a court order of this kind—one that forces decryption programming—is not discriminatory and is almost certainly a content-neutral regulation. If so, intermediate scrutiny will apply.[371] This step, significantly more complicated, presents "grave" constitutional doubts[372] and should further persuade a court to avoid the First Amendment question.

### *b. Intermediate Scrutiny*

To pass intermediate scrutiny, government action must be tailored such "that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'"[373] Apple faces a substantial burden of having to rewrite code from scratch every time law

[362] *321 Studios*, 307 F. Supp. 2d at 1100 ("Plaintiffs argue that the DMCA, as interpreted by the Studios, regulates the computer code on the basis of its content, since it bans only the kind of speech (code) that indicates how to circumvent a technological measure that protects a copyright. As such, plaintiff argues, the strict scrutiny analysis applies.").

[363] *Id.*

[364] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 329 (S.D.N.Y. 2000), *aff'd sub nom. Corley*, 273 F.3d 429.

[365] 475 U.S. 41 (1986).

[366] *Reimerdes*, 111 F. Supp. 2d at 329; *see also Playtime Theaters*, 475 U.S. at 46–49.

[367] *Id.*

[368] *Id.*

[369] *Id.*

[370] Government's Motion to Compel, *supra* note 13, at 18–19 ("The government shares Apple's stated concern that 'information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission.' [But t]he Order at issue does not compromise that interest." (quoting *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [perma: http://perma.cc/8Y92-S555])).

[371] *See Reimerdes*, 111 F. Supp. 2d at 328.

[372] *See* United States *ex rel.* Attorney Gen. v. Del. & Hudson Co., 213 U.S. 366, 408 (1909).

[373] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 450 (2d Cir. 2001) (quoting Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 662 (1994) (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989))).

enforcement needs to access an iPhone during a criminal investigation.[374] Alternatively, Apple could keep the code, but doing so could require extraordinary efforts to prevent it from being breached and exploited.[375] Even the government has acknowledged this difficulty, which is why it suggested that the code may be destroyed after one use.[376]

This burden distinguishes the Apple case from the other code cases. In those cases, the courts found that the government regulations at issue survived the tailoring prong of intermediate scrutiny because restricting programmers from posting decryption code was an incidental restraint on speech.[377] Those examples, however, required inaction—the programmers were forbidden from posting code. Conversely, for Apple to comply with the government order, it must write code

Regarding the "government's legitimate interest," the FBI's application to Judge Pym based on the All Writs Act is likewise distinguishable from other code cases. In *321 Studios*, for example, the court evaluated whether Congress had a substantial government interest for enacting the DMCA.[378] Congress, according to the court, found that "the DMCA was needed to protect copyrights and intellectual property rights."[379] The *Elcom* court also explained that the legislative history of the DMCA demonstrated that Congress passed it to "promot[e] electronic commerce while protecting the rights of copyright owners."[380] The question for a court here might be framed as whether the All Writs Act—an ambiguous, little-known, facially incomprehensible statute from 1789—was passed with an interest in criminal justice so substantial as to justify Apple's forced decryption. Even if some legislative history were suggestive of certain intent, the question now is whether a modern court would care. The *New York Telephone* Court's creation of three discretionary factors to test the legitimacy of a writ issued under the All Writs Act suggests that this is unlikely.[381]

Suppose, instead, that a court would focus not on the 1789 legislature's interest in passing the All Writs Act but on the FBI's interest in demanding encryption code under the Act. The FBI would likely claim that its interest is in criminal justice, which may be a permissible government interest under intermediate scrutiny. Unfortunately in this case this interest is illegitimate and thus fails intermediate scrutiny. By creating a backdoor to its iPhone, Apple would be left exposed to criminal hackers seeking to undermine the security of

[374] *See* Apple's Brief, *supra* note 17, at 23–24.

[375] *Id.* at 25.

[376] *Id.* at 24.

[377] *See, e.g.*, 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1101 (N.D. Cal. 2004).

[378] *Id.* at 1099–1101.

[379] *Id.* at 1101.

[380] United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1124 (N.D. Cal. 2002).

[381] *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977).

the newly weakened iPhone.[382] Thus, the government's actions would undermine its interest rather than promote it.

The government should know all too well how easily exploitable encryption code is.[383] After all, its own Clipper Chip technology was undermined by hackers, which abruptly ended that proposal.[384] In looking at the previous DMCA cases, there is a certain irony. Congress enacted the DMCA to prevent decryption.[385] That is why the programmer in *Reimerdes*, for example, was prohibited from posting on his website decryption code that would bypass a DVD's anticopying technology.[386] The court there stated that protecting copyrighted works from the "vastly expanded risk of piracy in this electronic age" was a substantial government interest;[387] that "[o]nce a decryption program . . . is written, it quickly can be sent all over the world";[388] and that "[t]he spread of means of circumventing access . . . is analogous to a propagated outbreak epidemic."[389] Yet with Apple, the government would end up as the propagator. If the government forces Apple into a position where Apple's encryption code can be exploited, the government has not further criminal justice; it has opened the door to criminality. This means the government's claimed interest in compelling code is illegitimate, further complicates the "big question" of compelled code and the First Amendment.[390]

### C. All Writs Act

After the "big question" of the First Amendment and computer code has been identified, a court should interpret the All Writs Act in a way that avoids free speech issues.[391] Fortunately for Apple, interpreting the All Writs Act to not allow the FBI to force Apple to write code is the only possible interpretation to accomplish this. A court should determine that a statutory interpretation in favor of Apple is plausible and, therefore, avoid addressing the constitutional issue.[392] The alternative is for a court to find that the FBI (or another appropriate

[382] *See* Apple's Brief, *supra* note 17, at 25.

[383] *See* Blaze, *supra* note 68.

[384] *See id.*

[385] *Elcom*, 203 F. Supp. 2d at 1124.

[386] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

[387] *Id.* at 330.

[388] *Id.* at 331.

[389] *Id.* at 332.

[390] *See NAMUDNO*, 557 U.S. 193, 196 (2009).

[391] *Id.*

[392] *See* Kloppenberg, *supra* note 261, at 3. For example, in *Gregory v. Ashcroft*, 501 U.S. 452 (1991), voters approved a state constitutional provision imposing mandatory retirement for state judges at age seventy. *Id.* at 455–60. Judges sued under the federal Age Discrimination in Employment Act of 1967 (ADEA). *Id.* at 455. The Court faced the constitutional question of whether Congress's extension of the ADEA to state judges was within its power under the Commerce Clause. *Id.* at 464. The Court avoided this question entirely, however, by determining that the ADEA was not intended to cover state judges to begin with. *Id.* at 470.

governmental agency) has authority under the All Writs Act. Such a finding, however, would necessarily require addressing Apple's First Amendment defense, which a court will not do under the avoidance canon.[393] In Apple's case, a court should interpret the All Writs Act such that it does not provide the authority to compel code, which avoids the difficult First Amendment question.

This All Writs Act analysis should be executed through the *New York Telephone* test: closeness, burden, and necessity.[394] A textual interpretation would be nearly impossible and frankly unnecessary. First, the language is vague and ambiguous.[395] Second, before *New York Telephone*, federal courts struggled to develop a standard for a textual reading.[396] Third, the Supreme Court in *New York Telephone* acknowledged the difficulty attendant to a textual analysis and hence created a standard for future courts to apply.[397] Fourth, the government applies this test in justifying the issuance of writs, as was the case with Apple in San Bernardino.[398]

### 1. Closeness

Apple has at least a plausible argument under the first *New York Telephone* factor. Following San Bernardino, Apple argued that the "closeness" factor was not met because Apple does not own its customers' iPhones.[399] For this reason, *New York Telephone* and *Mountain Bell* are distinguishable because in both those cases the third-party companies owned the telephone lines to which the government wanted access.[400] Furthermore, the company in *United States v. Hall* also owned and had direct access to its customers' credit card records.[401] Ownership was important in those cases because it established that the third parties upon whom the government sought to impose writs were sufficiently close to the investigations.[402] Apple, on the other hand, does not own its customers' iPhones.[403]

Additionally, the FBI's argument that Apple is close to an investigation like this presents a slippery slope. By that logic, Apple would be "close" to absolutely

[393] The code cases all had to address the constitutional issues because the courts found that pertinent statutes covered the decryption code at issue. See *supra* Part II.B.2.b for a discussion of recent court decisions applying the All Writs Act. *Corley* addressed this fact directly. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001). The appellants argued that the court "should interpret the statute narrowly so as to avoid constitutional problems." *Id.* After finding that the statute was "not susceptible to the narrow interpretations urged by the Appellants," the court then considered the constitutional claims. *Id.* at 444.

[394] United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977).

[395] *See* All Writs Act §§ 234, 261, 262, 28 U.S.C. § 1651(a) (2012).

[396] See *supra* Part II.B.1 for a discussion of the varying applications.

[397] *N.Y. Tel. Co.*, 434 U.S. at 174–75.

[398] *See* Government's Motion to Compel, *supra* note 13, at 8–18.

[399] *See* Apple's Brief, *supra* note 17, at 20–23.

[400] *See N.Y. Tel. Co.*, 434 U.S. at 162; *Mountain Bell*, 616 F.2d 1122, 1124 (9th Cir. 1980).

[401] *See* United States v. Hall, 583 F. Supp. 717, 717 (E.D. Va. 1984).

[402] *See, e.g.*, *id.* at 720–21.

[403] *See* Apple's Brief, *supra* note 17, at 21.

every single investigation in which an iPhone is found. Considering how popular the iPhone is, it is hard to imagine a situation in which a suspect's iPhone is found and Apple is far enough removed that it would not be subject to a writ. Arguably, this same logic could be applied to a telephone company like those in *New York Telephone* or *Mountain Bell*. However, in those cases, the government had probable cause that the suspects were relying heavily on the telephone lines specifically to facilitate their gambling operations.[404] Following San Bernardino, though, the FBI's "probable cause" can be summed up as follows: the suspect had an iPhone, and since he used it before the crime, his use must have been related to the crime.[405] This highlights the slippery slope concern. There is simply no criminal investigation in which this line of reasoning would not be valid.

Apple's ownership argument does have one key flaw: Apple owns the software that operates the iPhone,[406] which suggests (as one might expect) a closer connection between Apple and the iPhones than that argued for by Apple. Thus, while Apple may not have a right to a customer's phone as a physical object, it exercises substantial control over its operation, unlike traditional manufacturers.[407] For example, an analog watch manufacturer cannot alter its customers' products remotely. Apple, however, can. Despite this, Apple's closeness argument—combined with the slippery slope issue—is a plausible statutory interpretation of the All Writs Act and subsequent *New York Telephone* factors. That is all that is needed under the constitutional avoidance doctrine.[408]

### 2. Burden

Apple has a strong argument under the second factor, and a judge should find the FBI's order burdensome. First, Apple has stated that complying with the order could require enlisting a team of engineers to work for a month.[409] Further, Apple may face criticism for complying with an order that directly contradicts its own privacy values.[410] This criticism could have a significant economic impact on Apple.[411] The order in *New York Telephone*, on the other hand, involved the "meager" assistance of installing the pen register.[412] Additionally, Apple may have to rewrite code from scratch every single time law enforcement needs to break into an iPhone.[413] Alternatively, Apple could keep

[404] *N.Y. Tel. Co.*, 434 U.S. at 162; *Mountain Bell*, 616 F.2d at 1124.

[405] *See* Government's Motion to Compel, *supra* note 13, at 1.

[406] *Id.* at 11.

[407] *See id.*

[408] *See* Hasen, *supra* note 256, at 192.

[409] Apple's Brief, *supra* note 17, at 13.

[410] *See* Maya Kosoff, *Why People Are Up in Arms over Google's New Messaging App*, VANITY FAIR: HIVE (Sept. 21, 2016, 12:44 PM), http://www.vanityfair.com/news/2016/09/why-people-are-up-in-arms-over-googles-new-messaging-app [perma: http://perma.cc/W3MC-TAU2] (discussing criticism faced by Google for employing a less stringent security system in than it originally promised).

[411] *See id.*

[412] United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977).

[413] *See* Apple's Brief, *supra* note 17, at 24.

the code, but that would require significant efforts to prevent it from being exploited and the phone's security breached.[414] If this is not an undue burden under *New York Telephone*, it is difficult to imagine what would be.

On the other hand, not all judges would agree that Apple's alleged burden is significant enough to satisfy the burden element.[415] Presiding over the San Bernardino case, Judge Pym, for example, found that the FBI did have the requisite authority to order Apple to aid in the investigation.[416] Additionally, the *Mountain Bell* court found that complying with the court order in that case did not require substantially more efforts than those required in *New York Telephone* due to Mountain Bell's more advanced technology.[417] However, finding an undue burden is at least plausible to warrant avoidance. The work required by Apple would without question far surpass the burden imposed on companies in other, similar All Writs Act cases.

### 3. Necessity

As for the third factor, it is true the government faces obvious necessity in the law enforcement context. While Apple may argue that there are other ways to acquire information relevant to a case besides accessing a recovered iPhone, this same argument was presented in *United States v. Hall*.[418] There, the court said that while there was more than one way to catch a fugitive, accessing his credit card records would materially help.[419] However, Judge Orenstein's decision in the *Apple New York Case* is indicative of a narrower perspective justifying a more stringent necessity requirement.[420] Judge Orenstein wanted to ensure that the government had pursued every possible avenue before asking Apple to write code.[421] This may seem like an extreme perspective, but when combined with the burden issue, it is a sensible requirement. Apple would have to utilize extraordinary efforts to undermine its own security system—in both the short and long term.[422] This, of course, was untrue of companies in other All Writs Act cases who, for example, simply had to install a single device on a phone line[423] or access their own credit card records.[424] If Apple must go to great lengths, so too should the government in demonstrating forced code writing is absolutely required in a criminal investigation.

[414] *Id.* at 25; *see supra* Part III.B.2.b.

[415] *See, e.g.*, *Mountain Bell*, 616 F.2d 1122, 1132 (9th Cir. 1980); *see also Apple San Bernardino Case*, No. ED 15–0451M, 2016 U.S. Dist. LEXIS 20543, at *3–4 (C.D. Cal. Feb. 16, 2016) (concluding that Apple would be permitted to argue that its compliance with the Order would be unreasonably burdensome).

[416] *Apple San Bernardino Case*, 2016 U.S. Dist. LEXIS 20543, at *1–2.

[417] *See Mountain Bell*, 616 F.2d 1122, 1127–28 (9th Cir. 1980).

[418] United States v. Hall, 583 F. Supp. 717, 721 (E.D. Va. 1984).

[419] *Id.* at 721–22.

[420] *Apple New York Case*, 149 F. Supp. 3d 341, 373–74 (E.D.N.Y. 2016).

[421] *Id.*

[422] *See* Apple's Brief, *supra* note 17, at 23–29.

[423] United States v. N.Y. Tel. Co., 434 U.S. 159, 159 (1977).

[424] *Hall*, 583 F. Supp. at 717.

This *New York Telephone* factor is admittedly more speculative than closeness and burden—those two elements remain relatively constant no matter the situation. That is, Apple's link to an investigation and the efforts required to write new code are the same regardless of whether the iPhone belongs to a small-time drug dealer or a suspected terrorist. Necessity, however, could vary. Where the FBI is almost certain that an iPhone has information about a coming terrorist attack, the necessity is obviously greater than where the FBI thinks it is possible an iPhone would lead them to a drug dealer's buyers. However, it is a plausible argument that even in a case of suspected terrorism, Apple's assistance is not so necessary as to require extraordinary efforts on its part to break into a seized iPhone. The extreme difficulties involved are well documented,[425] and the potential futility of this assistance should always be a consideration. In fact, when the FBI was ultimately able to break into the San Bernardino shooter's iPhone, it found no useful information whatsoever.[426]

### D. *Legislation*

If a future court rightly applies the doctrine of constitutional avoidance, Apple should win. The court will escape entanglement with a legislative issue by interpreting the All Writs Act in Apple's favor. This will undoubtedly ease the company's concerns as well as those of privacy advocates in general. The law enforcement community, however, will be alarmed—perhaps justifiably so. The exponential rise of encryption could render some technology totally inaccessible.[427] The District Attorney of Manhattan, for example, stated that he had nearly 300 lawfully seized iPhones that could not be investigated without Apple writing code to circumvent the phones' security features.[428] Former FBI Director James Comey revealed that at the end of 2016, the FBI had 1,200 lawfully seized devices that it could not access due to encryption.[429]

This is a problem. Congress must enact a new federal regulatory regime to balance privacy and speech interests on the one hand with criminal justice and national security interests on the other. The All Writs Act, due to its age, ambiguity, and varied application, cannot serve as the legal basis upon which law enforcement may gain access to data in the age of encryption.[430] Nor are there other current verifiable statutory options, which explains why the government

[425] *See* Apple's Brief, *supra* note 17, at 23–29.

[426] Robert Hackett, *So, Did the FBI Find Anything on That San Bernardino Shooter's iPhone?*, FORTUNE (Apr. 23, 2016), http://fortune.com/2016/04/23/fbi-iphone-san-bernardino-shooter/ [perma: http://perma.cc/94HV-W2HE].

[427] *Cf.* Jeff John Roberts, *Top Prosecutor Blasts Apple and Google over 270 Encrypted Phones*, FORTUNE (June 9, 2016), http://fortune.com/2016/06/09/vance-encryption [perma: http://perma.cc/PP5L-WM3N].

[428] *Id.*

[429] Sarah Betancourt, *James Comey Says FBI Couldn't Crack 1,200 Encrypted Devices*, DAILY BEAST (Mar. 8, 2017, 12:04 PM), http://www.thedailybeast.com/articles/2017/03/08/james-comey-says-fbi-couldn-t-crack-1-200-encrypted-devices.html [perma: http://perma.cc/U3VA-SBBH].

[430] See *supra* Part II.B for an explanation of the All Writs Act and its application to third parties.

has relied on the Act so substantially. The Communications Assistance for Law Enforcement Act (CALEA), for example, passed in the mid-1990s, was intended to address law enforcement's worsening technological paralysis.[431] While the name of the act may suggest applicability, the statute specifically exempts providers like Apple from mandatory compliance.[432] The government agreed that CALEA does not cover Apple, though for different reasons not relevant here.[433]

More recent legislative proposals plainly do not adequately balance the interests.[434] In 2010, President Obama supported legislation that would have expanded the government's surveillance authority to cover communication service providers like Apple.[435] The proposed legislation was never officially submitted,[436] but it would have required technology companies to remain technically capable of complying with court orders.[437]

In other words, the proposal would have mandated backdoors.[438] In April 2016, Senators Richard Burr (a Republican from North Carolina) and Dianne Feinstein (a Democrat from California) drafted an encryption bill in response to the clash between Apple and the FBI following San Bernardino.[439] This legislation was ominously titled the Compliance with Court Orders Act of 2016.[440] Some language in the bill suggested a more balanced approach: "Nothing in this Act may be construed to authorize any government officer to require or prohibit any specific design or operating system to be adopted by any covered entity."[441] But that assurance was superficial, and the bill was widely understood to be an effective mandate for backdoors.[442] Legislation such as this is certainly friendly to law enforcement. However, in forcing perpetual code writing, it presents dangerous First Amendment concerns.

The technology and law enforcement communities need to come together to pursue meaningful, balanced encryption legislation that respects both of their interests. This will undoubtedly be a challenge given the technical complexity of the subject as well as the passions it elicits. However, a judicial resolution that

[431] *See Apple New York Case*, 149 F. Supp. 3d 341, 354–55 (E.D.N.Y. 2016).

[432] *Id.*

[433] *Id.* at 355 (reciting the government's argument that CALEA applies only to data "in motion," whereas data on a cell phone is data "at rest").

[434] *See, e.g.*, Savage, *supra* note 69.

[435] *See id.*

[436] *See* Lichtblau & Benner, *supra* note 69.

[437] *See* Savage, *supra* note 69.

[438] Glenn Greenwald, *The Obama Administration's War on Privacy*, SALON (Sept. 27, 2010, 6:28 AM), http://www.salon.com/2010/09/27/privacy_11/ [perma: http://perma.cc/HHN2-DVDA].

[439] *See supra* notes 310–12 and accompanying text.

[440] *See supra* notes 310–12 and accompanying text.

[441] See *supra* notes 310–12 and accompanying text addressing the text of the Compliance with Court Orders Act of 2016.

[442] Andy Greenberg, *The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'*, WIRED (Apr. 8, 2016, 11:16 AM), http://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/ [perma: http://perma.cc/M6SZ-G9ZL].

avoids the First Amendment issue would not address the escalating encryption issue. Neither would a statutory measure that is quickly crafted in the aftermath of another crisis.[443]

The statute must be a product of careful and meticulous planning, respect for the Constitution, concern for law enforcement, and, most importantly, compromise. Despite their very public misgivings, Apple's Tim Cook and the FBI's James Comey agreed on one point: this problem is for the legislature and thus for the people to solve.[444] They are right, but the reasons are complicated.

## IV. CONCLUSION

The trajectory of the war between law enforcement and technology is defined by uncertainty, confusion, and speculation. In this way, the future will likely mirror the past. The All Writs Act, drafted over two hundred years ago, is vague and ambiguous.[445] For over a century, its application to third parties was, too. While for some time it appeared that *New York Telephone* and its factors provided clarity, recent court decisions, which have varied widely, suggest otherwise.[446] As for the First Amendment, the question of whether code is speech is simply unsettled—both in academia and in the legal system—as the Supreme Court has not addressed it. Apple is unsure of the extent to which it must comply with government orders.[447] The FBI is uneasy about its future law enforcement abilities given the growth of encryption.[448]

Despite the murkiness, one fact remains indisputable: these issues will clash again. The legal battle after San Bernardino did not provide the resolution the nation anticipated; the can was simply kicked down the road. When the forced encryption question resurfaces, a court should apply constitutional avoidance and refer this issue to the legislature. Congress is simply better suited to provide long-term clarity on this national debate. It should act sooner rather than later.

[443] President Obama warned about this type of hastened resolution. *See* Russell Brandom, *How San Bernardino Changes the FBI's War on Encryption*, VERGE (Mar. 29, 2016, 11:43 AM), http://www.theverge.com/2016/3/29/11325030/apple-fbi-iphone-hack-security-encryption-what-comes-next [perma: http://perma.cc/6BMH-E65M].

[444] Dyer, *supra* note 312.

[445] *See supra* notes 295–303 and accompanying text.

[446] See *supra* Part II.B.2.b for a discussion of recent court decisions applying the All Writs Act.

[447] *See supra* Part III.B.2.b.

[448] *See* Levy, *supra* note 63; *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 1 (2011) (statement of Valerie Caproni, General Counsel, FBI).