Catholic University Law Review

Volume 67
Issue 1 *Winter 2018*

Article 11

3-20-2018

Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection Against Compelled Speech

Adrianna Oddo

Being Forced to Code in the Technology Era as a Violation of the First Amendment Protection Against Compelled Speech

Cover Page Footnote

J.D., The Catholic University of America, Columbus School of Law, 2018; B.A., University of Pittsburgh, 2015. The author would like to thank Ms. Brighton Haslett for her guidance through the researching, writing, and editing process of this Note. The author is incredibly grateful for the support of her family and friends. Finally, the author would like to extend her thanks to *the Catholic University Law Review* for their assistance in publishing this Note.

BEING FORCED TO CODE IN THE TECHNOLOGY ERA AS A VIOLATION OF THE FIRST AMENDMENT PROTECTION AGAINST COMPELLED SPEECH

Adrianna Oddo[+]

On December 2, 2015, fourteen people were killed and twenty-one others were wounded when two assailants opened fire at the Inland Regional Center in San Bernardino, California.[1] Syed Rizwan Farook and Tashfeen Malik fired sixty-five to seventy-five rounds in the center before fleeing the scene.[2] Law enforcement received a tip about the suspects' location, which resulted in a police chase.[3] Following a shootout with the police, both suspects were killed and, "[t]he FBI investigated the mass shooting as an 'act of terrorism' and determined that the two killers were not part of any terrorist network or cell. . . ."[4] During its investigation, the Federal Bureau of Investigation (FBI) discovered the shooters' broken cell phones and it appeared as though the shooters attempted to destroy their digital fingerprints.[5] The massacre forced the nation to focus on terrorism and gun policy, but it later shed light on a more technical issue.[6]

In February 2015, two months into its investigation, the FBI encountered a problem accessing the information on the shooters' phones.[7] The FBI director informed Congress that after two months the FBI could not unlock the terrorists' phones despite diligent efforts to circumvent Apple, Incorporated's (Apple)

[+] J.D., The Catholic University of America, Columbus School of Law, 2018; B.A., University of Pittsburgh, 2015. The author would like to thank Ms. Brighton Haslett for her guidance through the researching, writing, and editing process of this Note. The author is incredibly grateful for the support of her family and friends. Finally, the author would like to extend her thanks to the *Catholic University Law Review* for their assistance in publishing this Note.

1. Larisa Epatko, *Everything We Know About the San Bernardino Shooting*, PBS NEWSHOUR (Dec. 3, 2015, 9:27 AM), http://www.pbs.org/newshour/rundown/everything-we-know-about-the-san-bernardino-shooting/.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardinoshooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html; *see generally* Jim Finkle & Dustin Volz, *U.S. Tech Companies Unite Behind Apple Ahead of Iphone Encryption Ruling In re Search of Apple iPhone*, REUTERS (Mar. 4, 2016), http://www.reuters.com/article/apple-encryption-google-facebook-idUSKCN0W527Y.

encryption technology.[8] The United States Department of Justice sought to obtain this information by ordering Apple to "disable the feature that wipes data on [an iPhone] after 10 incorrect tries at entering a password."[9] Apple vehemently resisted the Justice Department's order and the American public became divided over the legal implications of technology, privacy, and encryption.[10] Apple CEO, Tim Cook, expressed concerns and explained his dissent to the Justice Department's order in a letter to Apple customers.[11] Cook's main concern with rewriting encryption software was that it would create a "chilling" effect on the privacy of Apple consumers.[12] Apple bases its opposition on two arguments. The government does not have authority under the All Writs Act of 1789 to force Apple to unlock its phones, and compelling Apple to violate its company philosophy infringes on the right against compelled speech.[13]

Apple committed itself to do everything possible to protect customers' data and personal information.[14] To achieve this, Apple uses encryption software to protect the vast amounts of information consumers store on their iPhones and has additionally "put that data out of [its] own reach, because [it] believe[s] the contents of your iPhone are none of [its] business."[15] While the theory behind data encryption is good for consumers and their personal information, it presents a problem for law enforcement that may need to gain access to devices for

---

8. Dustin Volz & Mark Hosenball, *FBI Director Says Investigators Unable to Unlock San Bernardino Shooter's Phone Content*, REUTERS (Feb. 9, 2016), http://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A.

9. Nakashima, *supra* note 7.

10. 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. The divide even extends to the Obama administration itself where "some of the president's most senior aides are staking out a variety of positions on the issue." Although the administration repeatedly stated there is no "serious internal disagreement about policy," the actions of agency officials, such as the Director of the FBI and the Defense Secretary, indicate conflicting positions. Michael D. Shear & David E. Sanger, *Competing Interests on Encryption Divide Top Obama Officials*, N.Y. TIMES (Mar. 5, 2016), https://www.nytimes.com/2016/03/06/us/politics/competing-interests-on-encryption-divide-top-obama-officials.html.

11. Lichtblau & Benner, *supra* note 10; Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/; *Answers to your questions about Apple and security*, APPLE, http://www.apple.com/customer-letter/answers/ (last viewed Oct. 17, 2017).

12. Cook, *supra* note 11.

13. 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 14–15, 33–34, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (N.D. Cal. Feb. 25, 2016) (No. CM 16-10), 2016 WL 767457 [hereinafter Apple Inc.'s Motion To Vacate Order]; Adam Satariano, *Apple-FBI Fight Asks: is Code Protected as Free Speech?*, BLOOMBERG (Feb. 23, 2016), https://www.bloomberg.com/news/articles/2016-02-24/apple-fbi-fight-asks-is-code-protected-as-free-speech.

14. Cook, *supra* note 11.

15. *Id.*; *see also* Apple, Inc., *iOS Security* (May 2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

investigations.[16] After recognizing the issue that encryption presents, the government sought access to these devices by, among other routes, compelling Apple to write a "backdoor" to the iPhone through a court order.[17] Compelling companies to write new software for their products has First Amendment implications that courts need to address; however, every case that has made it to court has been dismissed before a ruling can be issued.[18] Without a decision or definitive answer regarding these investigations, consumers are unaware that the privacy, security, and safety of their devices may not be protected.[19]

Using a court order to compel Apple—or any company—to assist in an investigation is not necessarily illegal and alone does not violate any of the company's rights. But requiring Apple to create a backdoor to its software—something it is fervently and fundamentally opposed to—may violate the company's rights.[20] The First Amendment of the United States Constitution guarantees "Congress shall make no law . . . abridging the freedom of speech."[21] Since the First Amendment's passage in the late 1700s, American law has shaped and defined the protections and guarantees of the First Amendment.[22] Due to recent technological advancements, courts have held that computer code is speech and have provided guidance on the degree of protection that computer code is afforded.[23] Courts have also addressed ancillary speech matters, such as compelled speech and compelled affirmations, which further contemplate the nature of protections afforded to computer code as a matter of constitutional law.[24] The technological advancements of Apple's encryption software and the unique conundrum presented by attempting to gain access to their devices warrant an evaluation of the First Amendment in this context.[25] This evaluation is necessary not only with regard to an order creating a backdoor to Apple's product, but also with regard to requiring Apple to authorize the program to function on its devices despite Apple's fundamental opposition to everything that program stands for.[26]

---

16. Jeff John Roberts, *Locked Apple Devices are Piling Up in Police Evidence Rooms*, FORTUNE (Nov. 17, 2016), http://fortune.com/2016/11/17/locked-apple-devices-are-piling-up-in-police-evidence-rooms/.

17. Cook, *supra* note 11.

18. Satariano, *supra* note 13.

19. *See generally* Cook, *supra* note 11 (describing uncertainty and availability of data protection without definite legal precedent).

20. Satariano, *supra* note 13; Cook, *supra* note 11.

21. U.S. CONST. amend. I.

22. *See generally About the First Amendment*, http://www.firstamendmentcenter.org/about-the-first-amendment (last visited Oct. 26, 2017) (tracing the history of shaping and defining the protections guaranteed by the First Amendment).

23. Satariano, *supra* note 13.

24. *See generally About the First Amendment*, *supra* note 22 (describing ancillary speech matters covered by the courts).

25. Satariano, *supra* note 13.

26. *Id.*; *see generally* Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 1–3.

Not all speech is afforded the same protection under the First Amendment.[27] Cases throughout the past 200 years have determined what speech is and is not protected in addition to how much protection is actually given. Courts must ultimately consider the critical distinctions between pure speech and expressive conduct regarding whether computer code is speech.[28] With respect to questions regarding computer code, courts must further distinguish whether the speech in question is source code or object code.[29] Another caveat to the First Amendment is the fundamental right of the American people to be protected from government compulsion of any kind of speech.[30] Previous decisions surrounding computer code and compelled speech serve as a framework to analyze cases that arise due to recent technological advancements.

This Note discusses why, under First Amendment law, Apple should not be required to create code that circumvents its encryption software to assist the FBI in obtaining information stored on legally seized Apple products. It begins with a description of the relevant law surrounding the development of the Free Speech doctrine in regards to computer code. This Note then analyzes the distinctions the courts have recognized between source code and object code when assigning proper constitutional protections. Next, this Note explores compelled speech and compelled authorization in relation to the First Amendment. In light of the Supreme Court's precedent, this Note explores the FBI's reasoning for compelling Apple's assistance in gaining access to seized phones, and Apple's justifications for resisting those orders. Finally, this Note argues that the government violates Apple's First Amendment rights by compelling them to create a backdoor to its software encryption because it is both compelled speech and a compelled affirmation. Finding otherwise would have severe implications for the future of Americans' personal privacy and security.

---

27. Jorge R. Roig, *Decoding First Amendment Coverage of Comput. Source Code in the Age of Youtube, Facebook, & the Arab Spring*, 68 N.Y.U. ANN. SURV. AM. L. 319, 325–27 (2012).

28. *See generally* Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277, 1282–85 (2005) (considering arguments differentiating speech and conduct as speech); R. George Wright, *What Counts as Speech in the First Place?: Determining the Scope of the Free Speech Clause*, 37 PEPP. L. REV. 1217, 1221, 1251 (2010).

29. 2 MELVIN F. JAGER, *Trade Secrets Law* § 9:12 (Oct. 2016 ed.); Roig, *supra* note 27, at 327–28; *see also* Katherine A. Moerke, *Free Speech to a Machine? Encryption Software Source Code is Not Constitutionally Protected "Speech" Under the First Amendment*, 84 MINN. L. REV. 1007, 1017–19 (2000).

30. *See, e.g.*, Wooley v. Maynard, 430 U.S. 705, 717 (1977) (holding "New Hampshire may not require appellees to display the state motto"); West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 641–42 (1943). The Supreme Court recognized that "speech does not lose its protection because of the corporate identity of the speaker," indicating that Apple's speech is still guaranteed protection. Pac. Gas and Elec. Co. v. Pub. Utils. Comm'n of California, 475 U.S. 1, 16 (1986) (citing First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 777 (1978)).

I. THE ESTABLISHMENT AND ELUSIVENESS OF THE FUNDAMENTAL FREEDOM OF SPEECH

The United States Constitution was ratified in 1788 and "is the supreme law of the United States."[31] In addition to providing governance guidelines for the role of the Legislative, Executive, and Judicial branches, it set forth the relationships and rights between different states and the federal government.[32] Arguably, the most important and controversial part of the Constitution, today and at ratification, is the Bill of Rights, which contains the rights of the People.[33]

Five of the fundamental rights guaranteed to the People by the Bill of Rights are established in the First Amendment. The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech . . . ."[34] The Framers did not initially think these rights needed to be explicitly stated;[35] however, based on the expansive case law of the First Amendment it can now be argued otherwise.

Despite being ratified in 1788,[36] the Constitution remains the governing document followed by the United States today. While the language contained in the text remains the same, the meaning of those words has been expanded, narrowed, and applied in many different contexts.

One provision that has evolved significantly is the Free Speech Clause of the First Amendment that provides "Congress shall make no law . . . abridging the freedom of speech. . . ."[37] Over time the courts have been faced with the issue of what qualified as "speech" when the framers passed the First Amendment. The Supreme Court did not hear many First Amendment or freedom of speech cases during the 100 years following the Bill of Rights' ratification because a majority of "federal judges [found] that the Bill of Rights [did] not apply to the states."[38] Ratification of the Fourteenth Amendment ultimately led to an increase of freedom of speech cases tried in federal courts during the Twentieth Century.[39] This proliferation of freedom of speech issues continues in the courts today.

---

31. *The Constitution*, THE WHITE HOUSE, https://www.whitehouse.gov/1600/constitution (last visited Oct. 26, 2017).

32. *Id.*

33. *See generally* Wright, *supra* note 28, at 1219–21 (touching on constitutional controversies, which stem from the document's dearth of terminological definition); *see also The Constitution*, *supra* note 31 ("[T]he Bill of Rights contains rights that many today consider to be fundamental to America").

34. U.S. CONST. amend. I.

35. *See The Constitution*, *supra* note 31 ("One of the principal points of contention between the Federalists and Anti-Federalists was the lack of an enumeration of basic civil rights in the Constitution").

36. *Id.*

37. U.S. CONST. amend. I.

38. *First Amendment Timeline*, THE FIRST AMENDMENT CENTER, http://www.firstamendmentcenter.org/first-amendment-timeline (last visited Oct. 27, 2017).

39. *Id.*

A. The Expansion of the Definition of Speech in the Technology Era has Not Clarified Any Existing Uncertainty, it has Only Created New Ones.

For two centuries courts, judges, and scholars attempted to focus the definition of "speech" within the context of the First Amendment.[40] When it comes to determining the meaning of speech, there are varying opinions of what the First Amendment actually protects.[41] Despite this variance, it has been determined that "[e]ven dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection."[42] As technology continues to develop, courts face situations where this technology is using or creating a language, which may or may not be considered speech.[43] These technological advancements, especially in regards to computer coding, prompted courts to address whether computer code is or is not considered speech. As courts issue decisions on computer code cases, a common factor is their focus on the information that the code conveys.[44]

The Sixth Circuit found in *Junger v. Daley* that the First Amendment protects computer source code.[45] In *Junger*, a professor sought injunctive relief on First Amendment grounds to enable him to distribute encryption software through his class website.[46] To address the First Amendment claim, the court evaluated whether the code Junger wanted to post on his website had speech-like qualities.[47] While the case was in the District Court, the government distinguished source code from object code as it applies to First Amendment protection.[48] Source code is expressed in a type of coding language, which can be understood by people with relevant experience.[49] Object code is the computer

---

40. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 446 (2d Cir. 2001); *see also* Moerke, *supra* note 29, at 1010–18 (providing a preliminary overview of specific types of speech and conduct that have historically been protected by First Amendment Jurisprudence in addition to the analysis of when courts found government "abridging" the freedom of speech).

41. *See generally* Wright, *supra* note 28, at 1218–20 (explaining the need for a comprehensive analysis to determine what actually counts as speech under the First Amendment).

42. *Universal City Studios, Inc.*, 273 F.3d at 446.

43. *See generally* Moerke, *supra* note 29, at 1018–20, 1024–27 (discussing cases regarding source and object code as well as encryption in relation to the First Amendment).

44. *Id.* at 1025–27 (detailing how courts determined whether computer coding constituted speech based on the coded information's expression of ideas, like other forms of protected communication).

45. Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000). The lower court "found that encryption source code is not sufficiently expressive to be protected by the First Amendment[;]" however, after oral arguments, the 6th Circuit "reverse[d] the district court and remand[ed] this case for further consideration." *Id.*

46. *Id.* at 484.

47. *Id.* at 484–85.

48. *Id.* at 483 (explaining source code is a set of instructions written in "a specialized programing language, such as BASIC, C, or Java"); *see also* Roig, *supra* note 27, at 327 (indicating additional types of "language" in which source code can be used for communication, including "C++, Fortran, COBOL, Python, Perl, and Java").

49. *Junger*, 209 F.3d at 483.

instructions that direct a computer through a sequence of 0s and 1s.[50] The issue with this distinction is that source code must be transferred into object code for a computer system to understand it.[51] The issue became whether source code, which is what the encryption software was, was guaranteed First Amendment protections.[52]

In its opinion, the Sixth Circuit referenced a Supreme Court holding that "'all ideas having even the slightest redeeming social importance' including those concerning 'the advancement of truth, science, morality, and arts' have the full protection of the First Amendment."[53] The Court went further to explain that First Amendment protection also extends to symbolic conduct, including conduct that is considered expressive and functional.[54] In looking toward Supreme Court decisions, the Sixth Circuit ultimately decided that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programing . . . it is protected by the First Amendment."[55] The Sixth Circuit found that source code contains both expressive and functional features, which complicates the determination of First Amendment protection.[56] However, the court did not address the level of judicial scrutiny to be applied because Junger needed standing "to bring a facial challenge" to the statute that prohibits him from posting the encryption code on his website.[57] In a similar case to *Junger*, the District Court in *Bernstein v. U.S. Department of State* found that encryption code, which required the use of a computer source code, is considered speech.[58]

While the court in *Junger* considered the distinction between object and source code to determine the First Amendment, the court in *Universal City Studios, Inc. v. Corley*[59] conducted a different analysis but reached a similar conclusion regarding code as speech. The court in *Universal City Studios* first determined that "communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."[60]

---

50. *Id.*

51. *Id.*

52. *Id.* at 484.

53. *Id.* (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).

54. *Id.* (citing United States v. O'Brien, 391 U.S. 367 (1968)) ("This protection is not reserved for purely expressive communication. The Supreme Court has recognized First Amendment protection for symbolic conduct, such as draft-card burning, that has both functional and expressive features.").

55. *Id.* at 485. The court also analogized computer code to musical scores, noting that while many people cannot read musical compositions, musicians prefer to communicate through their music. *Id.*; *see also* Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N. D. Cal. 1996).

56. *Junger*, 209 F.3d at 484.

57. *Id.* at 485.

58. *Bernstein*, 922 F. Supp. at 1436 ("For the purposes of First Amendment analysis, this court finds that source code is speech.").

59. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001).

60. *Id.*

The Second Circuit briefly addressed source and object code when it determined that the distinction was not as relevant as the court suggested in *Junger*, asserting that the readable nature of code by programmers qualifies it as communications protected by the First Amendment.[61] Thus, an inquiry into "the ease with which [computer code] is comprehended" becomes irrelevant in determining whether First Amendment protects code.[62]

The court further found "a programmer might communicate through code: to another programmer" and that limiting the First Amendment protection afforded to code "would impede their exchange of ideas and expression."[63] Taking its analysis a step further, the *Universal City Studios* court contemplated the scope of the First Amendment protection in regards to the code's usage and purpose. While the petitioners argued source code should be treated as pure speech, the court did not agree.[64] The Second Circuit decided that code in this case was a combination of non-speech and speech based on the functional and expressive elements.[65] Unlike a recipe or blueprint that serve as instructions in specific fields, "computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the internet."[66] The scrutiny that applies to computer code as speech is less relevant to the topic of this Note, but the Second Circuit's holding that "computer code conveying information is 'speech' within the meaning of the First Amendment" is analytically critical for determining computer code's constitutional protection.[67]

B. Despite the Vague Definition and Spotty Application of the Term "Speech," Protection Against Compelled Speech is More Definite.

Although the Court continues to grapple with interpretation of the word "speech," it remains steadfast that the purpose of the First Amendment is to protect speech. Justice Jackson famously discussed a main concern of the First Amendment in *West Virginia State Board of Education v. Barnette*.[68] Writing for the majority, Justice Jackson held that the forced salute of the American flag

---

61. *Id.* at 446. The court emphasized that "the ease with which a work is comprehended is irrelevant to the constitutional inquiry." This supports the court's notion that the mere prospect of a programmer being able to understand such code makes it communicative, and is thus considered speech, regardless of its complex nature. *Id.*

62. *Id.*

63. *Id.* at 448–49.

64. *Id.* at 451.

65. *Id.*

66. *Id.* The court concedes that human interaction may be something as small "as a single click of a mouse," but nonetheless requires that computer code be evaluated based on its functional and expressive elements. *Id.*

67. *Id.* at 449–50; *see also* 16B C.J.S. *Constitutional Law* § 1122 (2017).

68. 319 U.S. 624, 642 (1943).

in the classroom was a constitutional violation of the First Amendment.[69] Justice Jackson went on to state, "[i]f there is any fixed star in our constitutional constellation, it is that no official . . . can prescribe what shall be orthodox . . . or force citizens to confess by words or act their faith therein."[70] This decision was the first of many dealing with conduct as compelled speech under the First Amendment.

In *Wooley v. Maynard*,[71] the Court considered compelled speech when Mr. Maynard and his wife sought relief because they found a New Hampshire law requiring license plates to display the state motto to be unconstitutional.[72] The Maynard's believed the New Hampshire motto, "Live Free or Die," to be morally, religiously, and politically against their beliefs as Jehovah's Witnesses.[73] The Supreme Court held "the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all."[74] The Court found that forcing an individual to publicly display an ideal that he or she finds fundamentally unacceptable violates that individual's Constitutional rights.[75] The Court asserted that the government may not restrict what the People say and further, that the government may not compel what "protects" the People–that is, "the right of individuals to hold a point of view different from the majority."[76] When the government compels speech, it "invades the sphere of intellect and spirit which it is the purpose of the First Amendment to our Constitution to reserve from all official control."[77]

The Court in *Wooley* then determined whether the state had a convincing reason to justify such compelled actions.[78] After considering the proffered governmental interest for enforcement of this statute, the Court began its conclusion by reasserting a previous holding, "even though the governmental purpose [was] legitimate and substantial, that purpose cannot be pursued . . . when the end can be more narrowly achieved."[79]

---

69. *Id.* Justice Jackson opines that the forced salute in this case not only exceeds the school board's authority, it "invades the sphere of intellect and spirit which it is the purpose of the First Amendment to our Constitution to reserve from all official control." *Id.*

70. *Id.*

71. 430 U.S. 705, 714 (1977) (citing *Barnette*, 319 U.S. at 633–34).

72. *Id.* at 707–08.

73. *Id.* at 707.

74. *Id.* at 714 (referencing *Barnette*, 319 U.S. at 633–34).

75. *Id.*

76. *Id.* at 715 (referencing *Barnette*, 319 U.S. at 642). The Court noted the importance of protecting varying viewpoints of all of its citizens, even those contrary to the majority, and the government must act consistent with such principles. *Id.* at 715.

77. *Id.* at 715 (quoting *Barnette*, 319 U.S. at 642).

78. *Wooley*, 430 U.S. at 716.

79. *Id.* (quoting Shelton v. Tucker, 364 U.S. 479, 488 (1960)). The Court went on to hold that "where the State's interest is to disseminate an ideology, no matter how acceptable to some,

The Court later recognized the limitations placed on the government when compelling corporations to speak in a manner inconsistent with the company's business principles and viewpoints. In *Pacific Gas and Electric Company v. Public Utilities Commission of California*,[80] the Court held that requiring Pacific Gas and Electric Company to distribute or carry a message it fundamentally disagreed with was unconstitutional.[81] The Pacific Gas and Electric Company was required to carry the message of the Public Utilities Commission in a newsletter that it distributed monthly to customers in their bill.[82] The Court found that corporate entities cannot be compelled to make statements that they disagree with[83] because the right to speak also provides the right not to speak, or in this case, publishing a message it disagrees with.[84]

C. Existing Law has Taken Protection Against Compelled Speech Further, and Grants Protection Against Compelled Oaths or Affirmations

The Court further expanded First Amendment protections against compelled speech in *Speiser v. Randall*.[85] This case dealt with a California tax exemption form, which allowed World War II veterans to receive a tax break so long as they provided an oath or affirmation that they would not advocate overthrowing the Federal or California state government.[86] Legal action ensued when some veterans were denied the exemptions because they submitted the forms without their oath or affirmation.[87] The veterans who were denied the exemption brought suit claiming the required oath or affirmation was a violation of their First Amendment rights.[88] The Court found that under those facts, requiring a claimant to provide an oath or affirmation was unconstitutional.[89]

Overall, First Amendment jurisprudence provides that computer code is speech, regardless of the type of scrutiny applied to the actual information being

---

such an interest cannot outweigh an individual's First Amendment right to avoid becoming the courier for such message." *Id.* at 717.

80. 475 U.S. 1, 16 (1986).

81. *Id.* at 18. Carrying this message not only "burdens appellant's First Amendment rights because it forces appellant to associate with the views of other speakers, [but also] because it selects [these] other speakers on the basis of their viewpoints." *Id.* at 20–21.

82. *Id.* at 6–7.

83. *Id.* at 16 (citing *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 777 (1978) (noting that speech made by a corporate entity is still granted First Amendment protection despite the characteristic of the speaker)).

84. *Id.*

85. 357 U.S. 513, 513–15 (1958).

86. *Id.* 514–15.

87. *Id.* at 515.

88. *Id.* The lower courts in this case did not allow the Veterans to take the exemption because they refused to complete the oath portion of the forms. The Supreme Court of California affirmed the lower courts' decisions, and rejected the constitutional arguments asserted by the veterans. *Id.* at 515 n.1.

89. *Id.* at 527–30.

conveyed. Thus, individuals cannot be compelled to create computer code because that would be considered speech. The law also illustrates that requiring a person to make an oath or affirmation is a form of compelled speech, and is thus per se unconstitutional.

II. THE IMPORTANCE OF A MORE INCLUSIVE DEFINITION OF SPEECH IN THE TECHNOLOGY ERA INCREASES AS AN ACT OF TERRORISM LEADS TO THE UNITED STATES GOVERNMENT COMPELLING A COMPANY TO "SPEAK" AGAINST ITS WILL.

Following the events of the December 2nd massacre, the FBI conducted its investigation in a manner consistent with a terrorist attack on United States soil.[90] The FBI seized an iPhone 5C, manufactured by Apple, pursuant to a valid search warrant for a black Lexus IS300 that was issued on December 3, 2015.[91] The iPhone was owned by the San Bernardino County Department of Public Health, who gave authorities consent to search the device which was used by Farook under his employment.[92] In conducting its search, the government sought any pertinent information regarding the shooters involvement in the massacre, including others they may have communicated with regarding planning and execution.[93]

Despite collaboration with Apple, the FBI was unsuccessful in searching the device because the iPhone was protected by a "user-determined, numeric passcode" and the phone's operating system had an "auto-erase function."[94] This function would permanently destroy any information on the phone after

---

90. Government's Ex Parte Application for Order Compelling Apple, Inc. to Assist Agents in Search, at 2–3, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 16, 2016) (No. 15-0451M), 2016 WL 680288 [hereinafter Gov't's Application for Order Compelling Apple to Assist]; *see also* Michael S. Schmidt & Richard Pérez-Peña, *F.B.I Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html (indicating that Tashfeen Malik's Facebook post pledging her "allegiance to the Islamic State" led the FBI to "treat[] the massacre as an act of terrorism.").

91. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 2–3. The FBI obtained Mr. Farook and Ms. Malik's electronic devices, including their computers and phones, believing they would "provide the best hope for reconstructing their communications and motives." Schmidt & Pérez-Peña, *supra* note 90. FBI Director James Comey indicated that they were "going through a very large volume of electronic evidence . . . that these killers tried to destroy and tried to conceal from us." *Id.*

92. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 3–5.

93. *Id.* at 4, 19. As part of its investigation, the FBI conducted searches on the "digital devices and online accounts of Farook and Malik" via multiple warrants. Based on these searches and the resulting information, the FBI believed that there was "relevant, critical communications and data on [the locked iPhone from] around the time of the shooting . . . [that] cannot be accessed by any other means known to either the government or Apple." *Id.*

94. *Id.* at 3–5; *see also* Volz & Hosenball, *supra* note 8 (demonstrating that the FBI was unable to access the locked phone after two months because of the encryption on the phone, which has been a persistent challenge for local law enforcement and national security investigators).

entering ten incorrect passcodes.[95] Apple has, on numerous occasions, assisted law enforcement in executing search warrants to obtain "unencrypted file content[s] from phones without [use of] the passcode."[96] However, Apple developed new software that was installed on the iPhone seized by the government.[97] Apple asserted several times that its new software is written differently, and a program to provide access without the passcode does not exist.[98]

Despite Apple's assertions, the government filed an application for an order to compel in the United States District Court for the Central District of California, seeking the court to order Apple's assistance in executing a search warrant to unlock the phone.[99] More specifically, "the government request[ed] that Apple be ordered to provide the FBI with a custom signed iPhone Software ("IPSW") file, recovery bundle, or other Software Image File ("SIF") that can be loaded onto the [iPhone]."[100] The government cited the All Writs Act as authority to compel Apple to assist.[101] In pertinent part, the government claimed that "[p]ursuant to the All Writs Act[[102]], the [c]ourt has the power, 'in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers.'"[103] Sheri Pym, U.S. Magistrate Judge, granted the government's order pursuant to the All Writs Act on February 16, 2016, which included a provision allowing Apple five business days to respond to the order if Apple determines compliance with the order to be unreasonably burdensome.[104]

---

95. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 3.

96. *Id.* In a post answering common consumer questions, Apple clarified that, "[f]or devices running the iPhone operating systems prior to iOS 8 and under a lawful court order, we have extracted data from an iPhone." *Answers to your questions about Apple and security*, *supra* note 11.

97. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 3–6. To protect phones from more frequent and sophisticated cyber-attacks, Apple "built progressively stronger protections into [its] products with each new software release, including passcode-based data encryption." *Answers to your questions about Apple and security*, *supra* note 11.

98. *See generally* Gov't's Application for Order Compelling Apple to Assist, *supra* note 90; *see also* Emily Field, *Apple Says it Cannot Unlock New Devices for Law Enforcement*, LAW360 (Oct. 20, 2015), https://www.law360.com/articles/716435/apple-says-it-can-t-unlock-new-devices-for-law-enforcement ("[T]here [is] no technical way [Apple] could comply with a government request to unlock and extract user data from a pass code-protected smart device if it's running the most up-to-date operating system, although it could possibly crack an older phone.").

99. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 2–3.

100. *Id.* at 3–5.

101. *Id.* at 1–3.

102. All Writs Act, 28 U.S.C. § 1651 (2012).

103. Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 11 (citing Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979)).

104. *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M, 2016 WL 618401, *1–2 (C.D. Cal. Feb. 16, 2016).

Apple filed a motion to vacate the order to compel on February 25, 2016.[105] Apple was concerned that "'[j]ust this once' and '[j]ust this phone' . . . [will lead to] multiple other applications for similar orders."[106] Furthermore, Apple expressed concern that "[o]nce the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound without so much as a congressional vote."[107] In refuting the order, which Apple vigorously opposed, Apple claimed that "[t]he All Writs Act . . . which the government bases its entire case, 'does not give the district court a roving commission' to conscript and commandeer Apple in this manner."[108] Apple stated that "[t]he order would violate the First Amendment" as the code sought by the government is "compelled speech and viewpoint discrimination in violation of the First Amendment."[109] Apple further asserted that decisions regarding protecting the personal safety and privacy of consumers "[are] for American citizens to make through the democratic process" rather than through the courts.[110]

After Apple filed its motion, tech industry leaders expressed their support of Apple in the encryption battle and filed legal briefs with the court on March 3, 2016.[111] These companies recognized the importance of Apple's argument against usage of the All Writs Act as well as Apple's argument regarding violation of free speech.[112] A common assertion throughout these briefs was the need for legislation to adequately address encryption and all of its related issues, as opposed to letting courts make a fragmented body of law through case-by-

105. Apple, Inc.'s Motion to Vacate Order, *supra* note 13, at 1.

106. *Id.*; *see also* Roberts, *supra* note 16. If it were left up to the District Attorney in Manhattan, New York, Apple's assistance in unlocking phones would not just be a one-time occurrence. Noting that the number of locked iPhones reaching his office recently quadrupled and gaining a way into these phones is crucial because "rape and murder cases are going unsolved because investigators can't access Apple's phones." Roberts, *supra* note 16.

107. Apple, Inc.'s Motion to Vacate Order, *supra* note 13, at 1.

108. *Id.*

109. *Id.* at 32.

110. *Id.* at 35. Tim Cook, CEO of Apple, suggested that the encryption discussion should be decided on Capitol Hill where national security and privacy interests could be decided appropriately. Claire Zillman, *Apple's Tim Cook Says the iPhone Encryption Debate Should Shift to Congress*, FORTUNE (Feb. 22, 2016), http://fortune.com/2016/02/22/apple-ceo-tim-cook-fbi-iphone/. He also asserted that "Apple would 'gladly participate' in . . . a commission or other panel of experts on intelligence, technology, and civil liberties, to discuss the implications for law enforcement, national security, privacy, and personal freedom." *Id.*

111. Finkle & Volz, *supra* note 7. Supporters included Amazon, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo. *Id.*; Robert Hackett, *Big Tech Companies Rally Behind Apple*, FORTUNE (Mar. 3, 2016), http://fortune.com/2016/03/03/tech-companies-rally-behind-apple-fbis-case-threatens-fabric-of-internet/.

112. Hackett, *supra* note 111. Many companies who support Apple agree that the government cannot "force companies to create new technology." *Id.*

case decisions.[113] Many industry entities desired for a solution "that applies equally to all holders of personal information," while allowing "tech companies [] to have the ability to build and design their products . . . [without] the government mandating" the manner in which companies must go about doing that.[114] To accomplish the requests of all interested parties, decisions must be made clear on underlying legal issues to allow legislation to move forward.

III. SPEECH IS STILL SPEECH, REGARDLESS OF THE LANGUAGE IT IS SPOKEN.

The issue of whether compelling a company to write a computer program providing the government with access to information on its devices violates the First Amendment has never been addressed. Before the courts could rule on the merits of Apple's case regarding the San Bernardino massacre and the iPhone in question, the government found an alternative way to access the information on the cell phone.[115] However, just because the government no longer needs assistance to circumvent encryption software such as in this case, that does not make this issue an anomaly.[116] In fact, since the battle between the FBI and Apple became public, Manhattan District Attorney Cyrus Vance, Jr. claims there

---

113. *Id.*; *see also* Alina Selyukh, *The Apple-FBI Debate Over Encryption: A Year After San Bernardino and Apple-FBI, Where are we on Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption. Tech industry leaders are not the only ones expressing support for legislation, rather than judicial action, addressing encryption and privacy. A few months after the San Bernardino attack, FBI director James Comey commented:

> [T]his case . . . highlight[s] that we have . . . new technology that creates a serious tension between two values we all treasure—privacy and safety. That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living. It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before.

Press Release, Federal Bureau of Investigation Director James Comey, FBI Director Comments on San Bernardino Matter (Feb. 21, 2016), https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter.

114. Finkle & Volz, *supra* note 7. Many of Apple's supporters asserted the same arguments as Apple did in its motion to vacate. This included the improper use of the All Writs Act as a means for the government to accomplish the desired outcome, the "slippery slope argument," and arguments about setting dangerous precedent. Hackett, *supra* note 111.

115. Laurie Segall, Jose Pagilery, & Jackie Wattles, *FBI Says it has Cracked Terrorist's iPhone Without Apple's Help*, CNNMONEY (Mar. 29, 2016), http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/.

116. *See generally In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 374–76 (E.D.N.Y. 2016); Lichtblau & Benner, *supra* note 10; *see also* Kevin McCoy & Kevin Johnson, *U.S. Demands Apple Unlock Phone in Drug Case*, USA TODAY (Apr. 10, 2016), http://www.usatoday.com/story/news/2016/04/08/justice-moving-forward-separate-apple-case/82788824/ (explaining that the Department of Justice is pursuing legal action against Apple, even after the disposition of the legal battle regarding the San Bernardino massacre, to obtain its assistance in accessing an iPhone involved in a New York City Drug Conspiracy case).

are currently 423 Apple devices that are part of investigations that cannot be cracked.[117]

The scope of this Note limits the analysis to the legality of the court's original Order to Compel while considering First Amendment concerns of compelled speech and compelled affirmations.[118] In this case, the order requires Apple to create new software to get around their encryption software, and then add its "digital signature," both of which are violations of the First Amendment.

A. Not the Threshold, but a Consideration: is the Software Program Object or Source Code Speech?

Apple asserts that the government's order violates the First Amendment by compelling speech,[119] which is consistent with previous holdings. In *Junger*, the court held that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programing, . . . it is protected by the First Amendment."[120] The *Junger* court relied on the undisputed fact that encryption source code can convey information and that it can be read and understood by individuals familiar with programing language for informational purposes.[121] Similarly, in *In re of the Search of an Apple iPhone*,[122] the code sought by the FBI had the same expressive values. The FBI sought a code for software that removes security features and that additionally creates code within the operating system to bypass the encryption.[123] The possibility that this code can be understood and interpreted by anyone with proper experience supports the assertion that, like the code in *Junger*, the code sought by the FBI is source code, warranting First Amendment protection.

In further support of source code's expressive value, Apple highlights that development of the code sought by the FBI presents a threat to data security due to the likelihood that people other than Apple and the government will obtain the code and access consumer information.[124] More specifically, Apple is concerned with hackers obtaining the code. With this information, hackers could successfully bypass Apple's encryption and security features to gain access to iPhones.[125] The possibility that another person could understand the code is consistent with the court's analysis in *Universal City Studios*, which deemed

---

117. Roberts, *supra* note 16.

118. *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451M, 2016 WL 618401, at *1–3 (C.D. Cal. Feb. 16, 2016).

119. Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 2.

120. *Junger*, 209 F.3d at 485; *see also* Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) (analogizing music and mathematical equations to computer code).

121. *Id.* at 483.

122. Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 1–2.

123. *Id.* at 2–3.

124. *Id.* at 1–2; Cook, *supra* note 11.

125. Cook, *supra* note 11; Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 1–2, 17.

source code to be speech, requiring its protection.[126] Apple's fears alone justify and support the assertion that the code sought by the government has expressive, speech-like values demanding protection under the First Amendment.

B. The Government Cannot Compel Apple to Write Code Because it is Considered Speech

Apple correctly asserts that the government cannot compel it to create code based on First Amendment precedent. In *Wooley v. Maynard*, the Supreme Court held "the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all."[127] The Court held that forcing an individual to publicly display an ideal which he or she finds fundamentally unacceptable violates that individual's constitutional rights.[128] Apple dissented on several occasions in this case, including in a message to its customers and in its Motion to Vacate the Order.[129] In its message to customers the company states that "[w]e have no sympathy for terrorists" but went on to give its reasons why it fundamentally contests the government's demands.[130] The letter refers to Apple's compliance "with valid subpoenas and search warrants" that Apple is capable of assisting with.[131] Apple claimed that "[t]he government is asking Apple to hack [Apple's] own users and undermine decades of security advancements that protect [its] customers."[132] The government's inability to cite precedent or otherwise justify the expansion of its authority supports Apple's opposition. As justification, Apple argued that "this demand would undermine the very freedoms and liberty our government is meant to protect." Apple opposes the order because it does not believe in assisting the United States government to overreach its authority.[133]

The strong language that Apple used indicates that, like the citizens of New Hampshire in *Wooley*,[134] Apple is opposed to creating this backdoor for the government. Consistent with the holding in *Wooley*, forcing an individual, or company in this case, to display to the public an ideal that is fundamentally

126. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 446, 449 (2d Cir. 2001).

127. Wooley v. Maynard, 430 U.S. 705, 714 (1977).

128. *Id.* at 715.

129. Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 2–3; Cook, *supra* note 11.

130. Cook, *supra* note 11.

131. *Id.*

132. *Id.*

133. *Id.* Apple also expressed concern for this decision's ramifications, such as surveillance of Apple devices recording conversations or tracking a user's location. *Answers to your questions about Apple and security*, *supra* note 11.

134. Wooley v. Maynard, 430 U.S. 705, 713 (1977).

unacceptable effectively violates his constitutional rights.[135] Thus, the government's compulsion order effectively violates Apple's rights.

C. The Government is Also Prohibited from Compelling Affirmations in Regard to Speech

To take Apple's argument a step further, even if the code itself is not considered speech, thereby rendering the argument moot, there is another argument to be made against compelled speech through affirmations. While the software the FBI requested is one form of speech, the digital signature that Apple would need to put onto that software in order for it to be functional is also a form of speech. The iOS system, which runs on the iPhone in question, was created with several layers of protection to ensure the highest possible level of security to consumers.[136] In order for a program to run on the iOS system, it must be "'signed' cryptographically by Apple using its own proprietary encryption methods."[137] The signature certifies that the program is authentic.[138] The signature, in a way, certifies that Apple approves the program and that it is consistent with Apple's standards and ideals as a company.[139] Similar to the government in *Speiser*, the requested order would require Apple to "provide the FBI with a custom *signed* iPhone Software ("IPSW") file . . ." specifically requiring Apple to sign the software the government intends to use.[140] In *Speiser*, the court found that it was unconstitutional to require veterans to submit an oath or affirmation in order to receive a tax exemption because it compelled the veterans to speak.[141] In the present case, the government is also requesting unconstitutional speech. It is requiring Apple to place a digital signature on software Apple does not agree with, which is a compelled affirmation, and is unconstitutional.

---

135. First Nat'l Bank of Boston v. Bellotti, 435 U.S. at 765, 776–77 (1978) (noting that corporate speech is still granted First Amendment protections); *id.* at 714; *see generally* Cook, *supra* note 11.

136. *See generally* Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 5–6, 32; *Answers to your questions about Apple and security*, *supra* note 11.

137. Apple Inc.'s Motion to Vacate Order, *supra* note 13, at 32.

138. *Id.* (noting without this authentication, the code could not operate on the device).

139. Kim Zetter, *Apple May Use a First Amendment Defense in that FBI Case. And it Just Might Work*, WIRED (Feb. 25, 2016), https://www.wired.com/2016/02/apple-may-use-first-amendment-defense-fbi-case-just-might-work/. Nate Cardozo of Electronic Frontier Foundation asserted that Apple's forced signature of the software sought is compelled speech. He asserted that "[i]n the computer security world the digital signature is affirmation that not only is this code genuine, but it's intended . . . [and] is represented as coming from [the entity providing the signature]." He further asserts that "[i]f Apple signs this [software tool], it's the computer version of Apple saying, '[y]es this is us; yes we meant to do this; and yes it's a genuine representation of our will.'" *Id.*

140. Speiser v. Randall, 357 U.S. 513, 528–29 (1958); Gov't's Application for Order Compelling Apple to Assist, *supra* note 90, at 7–8 (emphasis added).

141. *Speiser*, 357 U.S. at 528–29.

Consistent with the Supreme Court's holding in *Pacific Gas,*[142] the action sought by the FBI in this case violates Apple's First Amendment rights. In *Pacific Gas,* the Court found that when the company distributed a newsletter with specific additions and viewpoints, it appeared as though the company was endorsing, supporting, or affirming the views and information distributed in that pamphlet.[143] Similarly, by requiring Apple to create a software program and requiring Apple to sign it, the government is forcing Apple to assert to its customers that it supports the creation and use of such a program.[144] Such an order is unconstitutional.

IV. CONCLUSION

Apple's motion to vacate the order compelling Apple to assist agents in a search on First Amendment grounds is consistent with established precedent. The uncertainty in distinguishing different types of code, source or object, and the protections associated with those distinctions need resolutions to ensure that no constitutional rights are violated. Although the Supreme Court has not yet addressed the issue of compelling creation of software to bypass encryption, Apple's arguments address issues that are likely to reach the Court in the near future. Yet, courts may not be the best place to decide this matter. As technology rapidly advances, America needs to carefully consider future implications that compelling such speech might have on First Amendment law and on the rights of citizens.

142. Pac. Gas and Elec. Co. v. Pub. Utils. Comm'n of California, 475 U.S. 1, 20–21 (1986).
143. *Id.* at 15–16.
144. Zetter, *supra* note 139.