2022

Code Free or Die: Regulations of Computer Code and the First Amendment

Dawn C. Nunziato

GW Law School Public Law and Legal Theory Paper No. 2022-16
GW Legal Studies Research Paper No. 2022-16

Code Free or Die: Regulations of Computer Code and the First Amendment

Dawn Carla Nunziato

Code Free or Die: Regulations of Computer Code and the First Amendment

- Dawn Carla Nunziato[1]

I. Introduction

On December 2, 2015, a holiday party for local government health workers turned into the worst domestic terrorist incident in American history since September 11, 2001. An American-born man of Pakistani descent, Syed Rizwan Farook, and his Pakistani-born wife, Tashfeed Malik, used an arsenal of semi-automatic pistols, rifles, and tactical gear to carry out the attack, at which they fired on workers and other attendees at a San Bernardino County, California Department of Public Health training event and holiday party. The mass shooting in San Bernardino killed fourteen people and injured more than twenty others.[2] The shooters were able to escape the scene, leaving pipe bombs in their wake, and carrying with them thousands of rounds of ammunition in their vehicle. Hundreds of law enforcement officials stepped in to catch the terrorists on the loose and investigate the incident. A tip informed them that Farook had left the party early; they were able to track down his rented Ford Expedition sports utility vehicle and identify the home that he and his wife rented in Redlands, California. Law enforcement officials located the couple and a gun battle ensued, leaving both terrorists dead.[3]

---

[1] Professor of Law, The George Washington University Law School. I am very grateful to Ken Rodriguez for providing library assistance in connection with this essay.

[2] See Adam Nagourney, Ian Lovett and Richard Perez-Pena, San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead, N.Y. Times, Dec. 2, 2015.

[3] See Krishnadev Calamur, Marina Koren, and Matt Ford, A Day After the San Bernardino Shooting, The Atlantic, Dec. 3, 2015.

While the horrific shooting and aftermath dominated several news cycles and generated debate over immigration policy, gun control, and terrorism, law enforcement's subsequent investigative efforts implicated even more far-reaching issues. Months after the shooting, the FBI sought to enlist Apple in its efforts to acquire potential evidence about the case by accessing the contents of the cell phone used by Syed Rizwan Farook. The FBI claimed that the messages, contacts, and other information stored on the cell phone could lead them to potential co-conspirators who assisted in the San Bernardino attack or who were involved in planning other terrorist activities, or other relevant evidence. The FBI's actions raised questions about the scope of the First Amendment and privacy that go to the heart of what free expression means in today's digital world.

The FBI claimed that it needed Apple's help because the cell phone in question, an iPhone 5c, operated Apple's iOS 9, and as such embodies a number of security features familiar to iPhone users, including passcode protections and encryption controls protecting the cell phone's contents. These passcode protections and encryption controls ensured that only the cell phone user himself – not Apple – is in possession of the access passcode, and further that: (1) the system could be programmed by the user to erase all of the cell phone's contents after ten unsuccessful attempts at guessing the user's passcode; (2) passcode attempts could only be entered manually, not by a computerized data entry process; and (3) the time delay between each unsuccessful passcode attempt was increased after each such attempt, to the point where after enough unsuccessful passcode attempts, this time delay would become infinite.[4] These iPhone iOS

[4] *See Order Compelling Apple Inc. to Assist Agents in Search, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203*, No ED 15-0451M (Feb. 16, 2016), Dkt. at 19 (the "Order").

security features frustrated the FBI's attempt to access potential evidence on the shooter's cell phone.

In order to improve the Government's likelihood of success in accessing the contents of the shooter's iPhone, the Department of Justice and the FBI sought to compel Apple to assist it in these efforts by securing a court order compelling Apple to write a software program that would defeat certain of the security features and encryption controls on the shooter's iPhone, as I discuss below. Apple claimed that the Order was an unwarranted exercise of the court's power under the All Writs Act, and further, that the Order violated Apple's First Amendment rights. In this essay, I briefly explore Apple's argument under the All Writs Act, and then turn to a detailed examination of Apple's First Amendment defense to the Government's Order. I argue that, notwithstanding the fact that the government sought to compel Apple to engage in the production of computer code -- code that may incorporate expressive elements -- it is not clear that the government in this case was compelling Apple to engage in protected expression, nor that the Government Order in this case embodied a content-based or a viewpoint-based regulation of or compulsion of speech. First, as the applicable precedent makes clear, although a government regulation

[67] *Id.* at 61.
[68] *Id.* at 62.
[69] *Id*. at 64.

of computer code *may* target such computer code because of its content, it may also target such computer code based on its functionality and without reference to its content. In the Apple case, the government was not "concerned with whatever capacity [the source code at issue] might have for conveying information to a human being, and *that capacity . . . is what arguably creates a speech component*…." Rather, the Government Order compelled the creation of computer code "solely because of its capacity to instruct a [device] to decrypt [and] *[t]hat functional capability is not speech within the meaning of the First Amendment*." Because the Order at issue targets computer code solely because of its functional capability "without reference to the content of the regulated speech," the Order should be analyzed as a content-neutral regulation with an incidental effect on speech (and therefore subject to, at most, intermediate scrutiny under the First Amendment). Therefore, the reviewing court should subject the Government's Order to the intermediate scrutiny applicable to content-neutral regulations that have incidental effects on expression as set forth in *Turner Broadcasting Systems v. Federal Communications Commission*, and should consider whether the Order served as substantial government interest that is unrelated to the suppression of free expression and whether the incidental restriction on speech burdened more speech than necessary to further that interest. In applying this test, the court should hold that the government interest in this case – to secure potential evidence related to a terrorist attack – is substantial and that the means used by the government – compelling Apple to produce source code to enable the government to access such potential evidence -- while financially burdensome to Apple, does not substantially burden Apple's free speech rights, and as such, does not burden substantially more speech than is necessary to further that interest.

II. The Government's Order

The Government requested, and secured, an *ex parte* order from a magistrate judge of the U.S. District Court for the Central District of California to compel Apple to provide "reasonable

technical assistance to assist law enforcement agents in obtaining access to the data" on the shooter's iPhone.[5] The Order defined such "reasonable technical assistance" to include Apple's creation of a new version of the iPhone operating system that can be loaded on the iPhone in question to perform the following three functions that would assist the Government in attempting "brute force" or computerized trial and error passcode generation and entry to defeat the security protections on the iPhone and ultimately to access the contents of the cell phone.

The order required Apple to develop operating system software that would: (1) disable or bypass the iPhone's "auto-erase" function that its user may have activated – which, if activated, would result in the deletion of all data on the iPhone after ten unsuccessful passcode attempts by the

[5] *See* Order, *supra* note 4.

Government; (2) disable or bypass the requirement that passcode attempts be entered manually -- so as to enable the FBI to generate and submit potentially millions of passcode attempts via computerized methods; and (3) to remove the escalating time delays imposed after incorrect passcode attempts and thereby enable the FBI to repeatedly electronically submit passcode attempts without interposed delays. Finally, the Government Order required Apple (4) to cryptographically sign the software using Apple's own proprietary encryption methods to signify that the software is a legitimate Apple product, so that the software can be run on an iPhone.

In short, the Government was not asking Apple to turn over the passcode to the shooter's iPhone – since the passcode is not in Apple's possession; instead, it was asking Apple to develop new software (indeed a new operating system) for the iPhone, which would create a "back door" for the government to access the secure, encrypted content on the iPhone in question (and presumably on other iPhones using the same iOS as well). Such software would enable the FBI to build a brute-force tool that is able to interface with the iPhone in question and to use computerized methods of trial and error to attempt to guess the passcode on the iPhone, without running the risk that the contents of the iPhone will be automatically erased and without being locked out after repeated unsuccessful attempts to guess the passcode.

III. Apple's Motion to Vacate

In its motion to vacate the Government's Order, Apple asserted two primary defenses: first, that that court did not enjoy the power under the All Writs Act to demand that Apple write such a software program, and second, that the Order violated the First Amendment by compelling Apple to engage in expression – writing computer code – with which it disagrees. In this essay, I briefly explore Apple's argument under the All Writs Act, and then turn to a detailed examination of Apple's First Amendment defense to the Government's Order.

A Apple's Argument Opposing the Court's Reliance on the All Writs Act to Compel the Relief in this Case

On February 16, 2016, the government filed an *ex parte* application and proposed Order asking the court to compel Apple under the authority of the All Writs Act[6] to assist in the government's investigation of the San Bernardino shooters by developing software that would perform the functions described above. The court granted this Order. In its motion to vacate the Order, Apple claimed, first, that the court did not enjoy the power under the All Writs Act to compel Apple to develop the software with the functionality and specifications required by the Government.

The All Writs Act confers on federal courts the ancillary authority to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of the law."[7] The plain text of the statute confers on federal courts the authority to issue orders where: issuance of the writ is "in aid of" the issuing court's jurisdiction; the type of writ requested is "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and the issuance of the writ is "agreeable to the usages and principles of law."[8] If a government application under the Act meets all three of these requirements, the court "may" issue the requested writ in the exercise of its discretion.[9] The Supreme Court has held that a court deciding whether to undertake discretionary action under the All Writs Act should consider three factors: (1) the closeness of the relationship between the person or entity to whom the writ is directed and

---

[6] 28 U.S.C. § 1651.
[7] 28 U.S.C. § 1651(a).
[8] *Id.*
[9] *See, e.g., Application of U.S. in Matter of Order Authorizing Use of a Pen Register*, 538 F.2d ~~956, 961 (2d Cir. 1976), rev'd~~ on other grounds; *United States v. N.Y. Tel. Co*., 434 U.S. 159 (1977); *Morrow v. District of Columbia*, 417 F.2d 728, 736 (D.C. Cir. 1969); *Paramount Film Distributing Corp. v. Civic Center Theatre, Inc*., 333 F.2d 358, 360 (10th Cir. 1964); *Chemical & Indus. Corp. v. Druffel*, 301 F.2d 126, 129 (6th Cir. 1962).

the matter over which the court has jurisdiction; (2) the reasonableness of the burden to be imposed on the writ's subject; and (3) the necessity of the requested writ to aid the court's jurisdiction.[10]

Although the All Writs Act grants limited authority to the courts to act in aid of their jurisdiction, it is not intended to serve as "a grant of plenary power to federal courts"[11] and does not authorize courts to engage in an "end run around constitutional and statutory law."[12] While the All Writs Act may be invoked by courts "to fill in a statutory gap that Congress has failed to consider," it may not be invoked to grant the government authority that "Congress chose not to confer."[13] As such, the function of the All Writs Act is as a "gap filler" – a source of interstitial authority, given the reality that Congress cannot reasonably be expected to anticipate every circumstance in which a court might need to act to vindicate the rights of the parties before it.[14] Accordingly, courts cannot rely on the Act to issue an order that is explicitly or implicitly prohibited under a federal statute.

Apple correctly contended that the All Writs Act was being wrongfully invoked by the court in this case because the court was invoking the Act not merely to fill in a statutory gap, but rather to grant the government authority that Congress expressly chose not to confer under the Communications Assistance for Law Enforcement Act (CALEA).[15] In enacting CALEA, Apple contended, Congress expressly chose *not* to allow the government to compel electronic

---

[10] *See N.Y. Tel. Co*., 434 U.S. 159, 174-78 (1977).
[11] *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979).
[12] *In the Matter of an Application of the United States of America for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel*., 849 F. Supp. 2d 526, 578 (D. Md. 2011).
[13] *In re Order Requiring Apple, Inc., to Assist in the Execution of a Search Warrant Issued by ~~this Court~~*, ~~No. 15-MC-1902,~~ 2015 WL 5920207, at *2 (E.D.N.Y. Oct. 9, 2015).
[14] *See, e.g., Harris v. Nelson*, 394 U.S. 286, 300 (1969) ("the purpose and function of the All Writs Act to supply the courts with the instruments needed to perform their duty").
[15] 47 U.S.C. § 1001 *et seq.*

communications service providers like Apple to design their technology or systems in a particular way to facilitate the government's efforts to acquire communications data. The Communications Assistance for Law Enforcement Act expressly provides that the Act:

> *does not authorize any law enforcement agency or officer –*
>
> (1) *to require any specific design of equipment, facilities, services, features, or system configurations* to be adopted by any provider of wire of electronic communications services, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.
>
> (2) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communications service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.[16]

Given the express language of CALEA providing that law enforcement agencies are not authorized to require providers of electronic communications services like Apple to adopt or provide any specific design of equipment, features, or system configurations, Apple wass correct in claiming that the Order in this case is not an instance of the Act's being properly invoked to fill a statutory gap, but was rather an instance of the Act's being wrongfully invoked to grant the government authority that Congress expressly chose not to confer in the Communications Assistance for Law Enforcement Act.

In construing the All Writs Act, courts have further held that orders pursuant to the Act must meet the following two-part test: such orders must not (1) "adversely affect the basic interests of the … party" and they must not (2) "impose on undue burden" on the party subject to the order.[17] Apple correctly claims that, because it has a strong interest in maintaining its data security systems, the Government's Order – which compels it to defeat those security systems – adversely affects Apple's basic interests and therefore violates the first prong of the test for court

---

[16] 47 U.S.C. § 1002(b)(1) ("Design of features and systems configurations") (emphasis added).
[17] *United States v. Hall*, 583 F. Supp. 717, 719 (E.D. Va.1984).

orders under the All Writs Act. Second, and more importantly, Apple claims that because the successful development of the software required under the Order would require Apple to dedicate six to eight computer programmers' time for two to four weeks, the Government's Order imposes an undue burden on Apple, thus violating the second prong of the test for court orders under the All Writs Act. This burden is further increased by the Government's suggestion that, once Apple had created the requested software and the Government implements the software, Apple should then be required to delete the software and erase all traces of it. Because Apple would arguably be compelled to do the same thing over and over again -- given that there are hundreds of similar state and local government demands for Apple to create similar software for state and local governments to deploy on other iPhones that they hold in custody in connection with other investigations[18] -- the government's suggestion that Apple repeatedly create and then destroy such operating system software renders this Order particularly burdensome.

In summary, Apple's argument that the All Writs Act was improperly invoked by the court was valid because (1) the Act was not being invoked to fill a statutory gap, but rather to effect an end-run around statutory law and to grant the government authority that Congress expressly chose not to confer in the Communications Assistance for Law Enforcement Act (CALEA), and (2) the Order improperly imposed an undue burden on Apple and adversely affected Apple's basic interests in providing security for its products.

III.B. Apple's Argument that the Government's Order Violates the First Amendment

In its motion to vacate, Apple further contended that the Government's Order that Apple develop software to perform functions that would neutralize the safety features that Apple has built

[18] See Apple's Motion to Vacate at 3 and 24 (Manhattan District Attorney Cyrus Vance, Jr., has stated that the federal and state governments seek access to every iPhone currently implicated in ongoing criminal investigations, while officials in Sacramento, California have hundreds of

iPhones for which they would like to secure Apple's assistance in gaining access).

into iPhones[19] violated the First Amendment because this was tantamount to compelling Apple to speak. Apple's First Amendment argument essentially proceeds in three parts: first, the computer code the Government was compelling Apple to write constitutes speech that is protected by the First Amendment; second, the Government's Order compelling Apple to write computer code constituted compelled speech; and third, such compelled speech constituted a content-based or viewpoint-based restriction or compulsion that is subject to exacting judicial scrutiny. While the first prong of Apple's First Amendment argument rests on solid jurisprudential grounds, the second and third are on shakier foundation, as I explore below.

III.B.1. Computer Code Constitutes Protected Expression When Used For Expressive Purposes

Apple's argument that computer code constitutes speech within the ambit of the First Amendment's protections stands on solid -- if recent -- First Amendment foundations. In a series of cases involving the regulation of encryption and decryption software in the past two decades, courts analyzing the question of whether computer code is within the scope of the First Amendment's protections have answered in the affirmative – first with respect to human- readable source code written in languages like Pascal and C++, and then with respect to machine-readable object code as well.[20] However, courts have held that the level of scrutiny

---

[19] To recap, the Government Order at issue in this case requires Apple to develop operating system software that would: (1) disable or bypass the iPhone's "auto-erase" function that users can opt to select such that all data on the phone is deleted after ten unsuccessful passcode attempts; (2) disable or bypass the requirement that passcode attempts be made manually, so as to enable the FBI to electronically generate and submit potentially millions of passcode attempts via computerized methods; (3) to remove the escalating time delays imposed after incorrect passcode attempts and thereby enable the FBI to repeatedly electronically submit passcode attempts without interposed delays; and (4) to cryptographically sign this software using Apple's own proprietary encryption methods to signify that the software is a legitimate Apple product, so ~~that the software can be run on~~ an iPhone.

[20] See, e.g., *Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999); *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000); *Karn v. United States Department of State*, 925 F. Supp. 1 (D.D.C. 1996).

applicable to a particular government regulation involving computer code depends on whether the regulation targets the expressive components of the code or the functional components of the code at issue. While courts have held that pre-publication licensing schemes that restrict computer scientists' expression involving computer code bear a heavy presumption of unconstitutionality and trigger searching scrutiny under the First Amendment, they have also held that government regulations that target the functional, non-expressive aspects of computer code trigger intermediate scrutiny.

Beginning in the mid-1990s, courts have recognized that government regulation of computer code may trigger First Amendment scrutiny.[21] First, in a set of early cases that considered whether government export restrictions on computer scientists' dissemination of encryption software via the Internet implicated the First Amendment's protections, the courts answered in the affirmative. In the influential case of *Bernstein v. United States Department of Justice*,[22] for example, the Ninth Circuit was asked to determine whether government regulations that prohibited the dissemination of encryption source code via the Internet without a license constituted an unconstitutional prior restraint on protected expression. In that case, Daniel Bernstein, a computer scientist and professor, had developed a unique method of encrypting content -- "a zero-delay private-key stream encryptor based upon a one-way hash function"[23] -- that he described or instantiated in three formats: (1) in a paper written in English containing analysis and mathematical equations; (2) in source code, in two computer programs written in

---

[21] John P. Collins, Jr., Speaking In Code, 106 Yale. L.J. 2691 (1997); David McClure, First Amendment Freedoms and The Encryption Export Battle: Deciphering The Importance of Bernstein v. United States Department of Justice, 79 Neb. L. Rev. 465 (2000); James J. Carter, The Devil and Daniel Bernstein: Constitutional Flaws and Practical Fallacies in the ~~Encryption Export Controls, 7~~6 Or. L. Rev. 981 (1997) (discussing cases in which courts consider First Amendment protections for computer code).

[22] *Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999).

[23] *Id.* at 1135-36.

the high level programming language "C"; and (3) in a set of instructions in English, which explained how to program a computer to encrypt and decrypt data utilizing a one-way hash function, which essentially translated the source code into prose form.[24]

Professor Bernstein sought to present this scientific work product on encryption within his academic and scientific communities in order to facilitate academic exchange and peer review of his research.[25] Accordingly, he first sought to determine whether he needed to secure a license from the government before publishing his work product on the Internet.[26] The State Department responded that Bernstein's encryption programs constituted "munitions" under the then-applicable International Traffic in Arms Regulations, which regulated encryption technology, and that therefore Bernstein would need to secure a license in order to publish the paper, the source code, or the instructions version of his scientific work on the Internet.[27] The authority to grant or deny a license for disseminating encryption software was later transferred from the State Department to the Commerce Department, which was vested with the authority to determine whether to grant or deny such licenses, based on whether the grant would be consistent with "U.S. national security and foreign policy interests"[28] – with no further guidance or restrictions placed on the discretion of the licensing authority.[29]

---

[24] *Id*. at 1136.
[25] *Id.*
[26] *Id.*
[27] *Id.* In December 1996, President Clinton shifted licensing authority for nonmilitary encryption commodities and technologies from the State Department to the Department of Commerce. See Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996). The Department of Commerce then promulgated regulations under the Export Administration Regulations to govern the export of encryption technology, regulations administered by the Bureau of Export Administration ("BXA"). See 61 Fed. Reg. 68,572 (1996) (codified at 15 C.F.R. Pts. 730-74). Bernstein ~~subsequently amended his com~~plaint to add the Department of Commerce as a defendant, advancing the same constitutional objections as he had against the State Department. *Id.* at 1136.
[28] 15 C.F.R. S 742.15(b)
[29] 176 F.3d at 1138.

Professor Bernstein challenged the export regulations' licensing scheme as a facially invalid unconstitutional prior restraint on speech that vested unbridled discretion in the licensing authority.[30] In evaluating his challenge, the Ninth Circuit was first required to determine whether the material regulated under the licensing scheme at issue had "a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks."[31] Bernstein had contended, with the support of numerous declarations from cryptographers and computer scientists, that cryptographic ideas and algorithms were most usefully and precisely expressed and exchanged among scientists in source code form, because expressing their ideas in this form enabled scientists to convey their ideas with the precision and mathematical rigor that was impossible to achieve otherwise, and because expressing their ideas in source code form greatly facilitated the peer review and analysis of such ideas.[32] The court was persuaded by Bernstein's claims that computer scientists use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs, and that computer scientists utilize source code, among other reasons, in order to facilitate the precise and rigorous expression of complex scientific ideas.[33] Accordingly, the court held that encryption software, in its source code form, "must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine."[34] Because the licensing scheme at issue vested unbridled discretion in the government to grant or deny a license based on the discretion-less standard of whether the grant would be

[30] *Id.* at 1138.
[31] *Id.* at 1139.
[32] *Id*. at 1141.
[33] *Id.*
[34] *Id*. at 1141.

consistent with "U.S. national security and foreign policy interests,"[35] the court held that the licensing scheme was subject to strict scrutiny as a prior restraint on protected expression, and held the scheme to be invalid under such strict scrutiny.[36] Several other courts that were called upon to evaluate government licensing schemes on encryption software reached the same result as the *Bernstein* court, holding that encryption source code used by computer scientists to express their scientific ideas constituted protected expression and that such pre-publication licensing schemes embodied unconstitutional prior restraints.[37] These courts noted, however, that even though the pre-publication licensing schemes of encryption source code at issue were unconstitutional prior restraints, the same code might be made constitutionally subject to regulations that did not embody the evils of a system of prior restraints.[38]

Later courts have been asked to consider whether machine-readable *object code* – composed solely of 1s and 0s – constituted speech that was cognizable within the First Amendment's protections, and whether such code could be constitutionally made subject to regulations that targeted the functional instead of the expressive aspects of such code. In *Universal City Studios v. Corley*, which involved a statutory regulation of decryption software that did not embody a pre-publication licensing scheme, the Second Circuit was asked to rule on the constitutionality of the provisions of the Digital Millennium Copyright Act that penalized the dissemination of software designed to circumvent encryption controls used by copyright owners to control access to and copying of their digital works.[39] Eric Corley, who ran the hackers' website 2600.com, argued that he had a First Amendment right to post, and provide links to, both

---

[35] 15 C.F.R. 742.15(b)
[36] *Id.*
[37] *See also Junger v. Daley* and *Karn v. United States*, supra note 20.
[38] *See, e.g., Bernstein*, 176 F.3d at 1139.
[39] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

the source code and object code versions of DeCSS software, which was designed to circumvent the encryption controls used by movie studios to prevent unauthorized access to and copying of their copyrighted films stored on DVDs.[40]

The *Corley* court first explained that the dual nature of computer code – the fact that it has the capacity to direct the functioning of a computer, as well as the capacity to convey information – did not deprive it of the First Amendment's protection. Notwithstanding the functional capabilities of computer code, the court explained, "it is the conveying of information that renders [computer programs] speech for purposes of the First Amendment.[41] Observing that many types of First Amendment protected speech – such as recipes, instruction books, and musical scores – are functional and dependent upon the use of devices or machines for their implementation -- the court explained that "computer programs are not exempted from the category of First Amendment speech simply because their instructions require the use of a computer."[42] Thus, the court explained that the functional nature of computer code does not withdraw it from the protections of the First Amendment. The *Corley* court explained further that, for purposes of the First Amendment, there were no relevant differences between source code – written in high level programming languages like Pascal or C++ – and object code that was written purely in 1s and 0s and readable (primarily) by machines. The court stated: "If someone chose to write a novel entirely in computer object code by using strings of 1s and 0s . . .

, the resulting work would be no different, for constitutional purposes, than if it had been written in English."[43] The *Corley* court held that what distinguished protectable from unprotectable expression was whether the expression could be used to communicate information or ideas –

---

[40] *Id.*
[41] *Corley*, 273 F.3d at 447.
[42] *Id.* at 447.
[43] *Id.* at 445-46.

even if it is used by only a few select experts for such communicative purposes. While expression written in an obscure foreign language like Sanskrit or in the symbols of a musical score – like expression written in object code – may not be understood by many people, it is the fact that such expression can be used by some for communicative purposes -- to convey information and ideas – that triggers the protections of the First Amendment.[44]

Having decided that computer code – including both source code and object code -- is "speech" within the meaning of the First Amendment, the Second Circuit went on to consider the scope of protection that the decryption code at issue enjoyed and the standard of scrutiny applicable to the provisions of the copyright statute regulating computer code in that case. The provisions of the Digital Millennium Copyright Act at issue prohibited the dissemination of software that could be used to circumvent encryption controls used by authors to protect access to and prevent unauthorized copying of works protected by copyright.[45] The question for the court was whether this type of regulation of computer code was a content-based regulation subject to strict scrutiny or a content-neutral regulation subject to intermediate scrutiny. The court explained, as a preliminary matter, that the threshold inquiry into whether the regulation is content-neutral or content-based is applicable regardless of whether what is regulated is expression, conduct, or "any activity that can be said to combine speech and non-speech elements."[46] Once a speech component of the regulated activity is identified, the court

---

[44] *Id.*

[45] See 17 U.S.C. § 1201(a)(2) (anti-trafficking provision of Digital Millennium Copyright Act, prohibiting manufacture or dissemination of technology that is "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work [protected by copyright]") and 17 U.S.C. § 1201(b)(1) (anti-trafficking provision of Digital Millennium Copyright Act, prohibiting manufacture or dissemination of technology that is "primarily designed or produced for the purpose of circumventing a technological measure that effectively protects a right of a copyright owner").

[46] *Id.* at 450.

explained, the relevant inquiry was whether the government regulation was "justified without reference to the content of the regulated speech."[47]

Eric Corley argued that the copyright provisions at issue regulated the computer code that he posted because of its content – because it contained a particular type of expression, i.e., algorithms for circumventing the technological measures used by copyright owners to protect their works – and that therefore the provisions were content-based and subject to strict scrutiny. The court, however, reiterated that computer code contained both expressive and non-expressive/functional elements and held that the copyright provisions at issue regulated computer code based on its non-expressive/functional elements. The court explained that the provisions of the Copyright Act at issue preventing the dissemination of decryption software were not "concerned with whatever capacity DeCSS might have for conveying information to a human being, and that capacity . . . is what arguably creates a speech component of the decryption code."[48] Rather, the copyright provisions at issue applied to the computer code posted by Corley "solely because of its capacity to instruct a computer to decrypt. *That functional capability is not speech within the meaning of the First Amendment*."[49] Finding that the regulation at issue targeted computer code solely based on its functional capability "without reference to the content of the regulated speech,"[50] the court held that the regulation was a content-neutral regulation with an incidental effect on speech, and was therefore subject to intermediate scrutiny. The court analogized the Digital Millennium Copyright Act's prohibition on decryption computer code to a restriction on trafficking in skeleton keys with words or slogans written on them, in which the restriction would be found to be a content-neutral restriction that targeted trafficking in skeleton

[47] *Id.* at 451.
[48] *Id.* at 454.
[49] *Id*. at 454 (emphasis added).
[50] *Id.* at 454.

keys because of the keys' capacity to unlock jail cells, regardless of the fact that the keys also possessed a speech component. Finding that the copyright provision at issue was similarly a content-neutral regulation of computer code based on its functional capabilities, the court analyzed the regulation under the intermediate scrutiny regime set forth in *Turner Broadcasting Systems v. Federal Communications Commission*, [51] and considered whether the regulation served as substantial government interest that was unrelated to the suppression of free expression and whether or not the incidental restriction on speech burdened more speech than necessary to further that interest. The court readily found that the government's interest in preventing unauthorized access to encrypted copyrighted material was a substantial interest that was unrelated to the suppression of free expression.

Apple was correct to point to cases like *Bernstein* and *Corley* in support of its claim that computer code falls within the protections of the First Amendment. However, as the Second Circuit's analysis in *Corley* makes clear, the fact that computer code contains expressive elements within the scope of the First Amendment's protection does not resolve the ultimate questions of what level of scrutiny is applicable to government action regarding such computer code and whether the government action is permissible under the First Amendment.

III.B.2. Is a Government Order Compelling Apple to Write Computer Code that Performs Specific Functions Compelled Speech that is Subject to Strict Scrutiny?

Apple contended further in its motion to vacate that the Government Order compelling it to write computer code that performs specific functions was compelled speech and that such compelled speech was a content-based and viewpoint-based restriction of speech subject to exacting constitutional scrutiny. As I explain below, although Apple was correct that government regulations compelling speech are subject to searching First Amendment scrutiny, it is not

[51] 512 U.S. 622, 662 (1994).

entirely clear that the Government Order compelling Apple to produce computer code amounted to a content-based (or a viewpoint-based) compulsion of speech that would trigger strict scrutiny. Because the government in this case was ordering Apple to write and produce computer code, and because computer code can be considered protected expression, Apple claims that the Government Order falls within the ambit of the courts' compelled speech jurisprudence. But the cases in which the Supreme Court has found government regulations compelling speech to violate the First Amendment are distinguishable from the Government Order in this case, as discussed below.

Beginning in the mid-twentieth century, the Supreme Court recognized that the First Amendment right to freedom of speech also extended to and protected the freedom not to speak – i.e., the freedom not to be compelled to utter or associate with beliefs or affirmations with which the speaker disagreed. In the original compelled speech case of *West Virginia State Board of Education v. Barnette*,[52] the Court considered and struck down a West Virginia statute that required all school students to salute the United States flag and recite the Pledge of Allegiance and imposed a penalty of expulsion from school for failure to comply. Plaintiffs brought suit to enjoin enforcement of the statute against Jehovah's Witnesses, who for religious reasons refuse to salute and pledge allegiance to the flag. The Court observed first that the flag salute and pledge require the "affirmation of a belief"[53] and that the compulsory flag salute and pledge unconstitutionally compel an individual "to utter what is not in his mind."[54] The Court observed:

> If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein. [T]he action of the local authorities in compelling the flag

[52] 319 U.S. 624 (1943).
[53] *Id.* at 633.
[54] *Id.* at 634.

> salute and pledge transcends constitutional limitations on their power and 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.[55]

Because the statute at issue required a particular "attitude of mind" and compelled an individual to utter what was not in his or her mind, it invaded the intellectual sphere of the individual by compelling speech in violation of the First Amendment.

The Supreme Court extended its compelled speech jurisprudence several decades later in another case involving the rights of Jehovah's Witnesses not to be forced by the government to associate themselves with beliefs or affirmations with which they disagree. In *Wooley v. Maynard*,[56] two Jehovah's Witnesses challenged a state statute that required all New Hampshire motorists to display the state motto "Live Free or Die" on their license plates. George and Maxine Maynard, who viewed the state motto as repugnant to their moral, religious, and political beliefs, covered up the motto on the license plates of their automobiles and were repeatedly fined under the statute. George Maynard was subsequently jailed for refusing to pay the fines. The Court considered whether the state was constitutionally permitted to require an individual to "participate in the dissemination of an ideological message . . . for the express purpose that it be observed and read by the public."[57] Because the state sought to compel individuals to participate in the dissemination of a particular ideological message, the Court subjected the statute to strict scrutiny, and held that it unconstitutionally infringed the Maynards' right not to be compelled to speak.[58] In striking down the statute, the Court explained that our system of free speech protects not only the right to speak but also the concomitant right not to speak, because "[a] system which

---

[55] *Id.* at 642.
[56] 430 U.S. 705 (1977).
[57] *Id.* at 713.
[58] *Id.* at 716.

secures the right to proselytize religious, political, and ideological causes must also guarantee the concomitant right to decline to foster such concepts."[59]

Later, in *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*,[60] the Court considered the lower courts' application of a Massachusetts public accommodations law to compel private parade organizers to include in their parade a group seeking to impart a message that the organizers did not wish to convey. The lower courts had interpreted the state public accommodations statute to require that the South Boston Allied War Veterans Council – a group of private parade organizers – include the Irish-American Gay, Lesbian and Bisexual Group of Boston (GLIB) in the St. Patrick's Day Parade that the Council organized. The Court ruled that the "state courts' application of the statute produced an order essentially requiring [the parade organizers] to alter the expressive content of their parade"[61] to include the pro-gay rights message of GLIB, which violated the First Amendment right of the organizers "not to propound a particular point of view."[62]

The Supreme Court, however, has limited the reach of its compelled speech/right not to speak jurisprudence in recent years, and has declined to extend this jurisprudence to instances where the actions that the government compelled were not sufficiently expressive or where the speaker could readily disavow his or her association with the speech that was compelled by the government. In *PruneYard Shopping Center v. Robins*,[63] shopping mall PruneYard and its owner Fred Sahadi challenged the constitutionality of the California Supreme Court's interpretation of the state constitution's free speech provisions to protect "speech and petitioning,

---

[59] *Id.* at 714.
[60] 515 U.S. 557 (1995).
[61] *Id.* at 572-73.
[62] *Id.* at 575.
[63] 447 U.S. 74 (1980).

reasonably exercised, in shopping centers [that] are privately owned."[64] The owner of The PruneYard argued that, as a private property owner, he enjoyed a First Amendment right not to be forced by the state to use his property as a forum for the speech of others or to be compelled to propound or associate with a particular viewpoint by serving as a forum for the speech of others. The Court rejected PruneYard's First Amendment challenge, explaining that there was little likelihood that the views of those engaging in expressive activities at the owner's shopping center would be identified with the owner, in light of the fact that the owner remained free to dissociate himself with those views and – unlike the challengers in *Barnette* and *Wooley* – was not "being compelled to affirm [a] belief in any governmentally prescribed position or view."[65]

Similarly, in the recent case of *Rumsfeld v. Forum for Academic and Institutional Rights*, the Supreme Court clarified and narrowed the reach of its compelled speech/right not to speak jurisprudence.[66] In that case, the Forum for Academic and Institutional Rights (FAIR) – an association of law schools and law faculties whose members had policies opposing discrimination based on sexual orientation – challenged the constitutionality of the Solomon Amendment, which withheld certain federal funding to schools that denied access to military recruiters because such recruiters discriminated on the basis of sexual orientation. FAIR claimed that the Amendment's act of compelling law schools to accept military recruiters on equal terms, and to speak on behalf of military recruiters (such as by announcing relevant information about recruitment efforts to their students), violated its members' First Amendment rights.

The Court rejected FAIR's First Amendment arguments. First, the Court explained that the Amendment's compulsion of recruitment assistance on behalf of military recruiters – e.g., by

---

[64] *Id.* at 78.
[65] *Id.* at 88.
[66] 547 U.S. 47 (2006).

requiring law schools to send emails to students on the recruiters' behalf – was "a far cry from the compelled speech in *Barnette* and *Wooley*," since there was "nothing in this case approaching a government-mandated pledge or motto that the school must endorse" and since the Amendment did not have the effect of dictating the content of the law school's speech.[67] The Court explained: "Compelling a law school that sends scheduling e-mails for other recruiters to send one for a military recruiter is simply not the same as forcing a student to pledge allegiance, or forcing a Jehovah's Witness to display the motto 'Live Free or Die,' and it trivializes the freedom protected in *Barnette* and *Wooley* to suggest that it does."[68] The Court further held that the Solomon Amendment did not unconstitutionally compel law schools to host or accommodate another speaker's message, distinguishing the Amendment at issue from the challenged statute at issue in *Hurley*. Unlike in *Hurley*, the Court explained, the Solomon Amendment's act of compelling law schools to accommodate military recruiters did not in any way alter the law school's own message: "Unlike a parade organizer's choice of parade contingents, a law school's decision to allow recruiters on campus is not inherently expressive. Its accommodation of a military recruiter's message is not compelled speech because the accommodation does not sufficiently interfere with any message of the school."[69]

Notwithstanding the fact that the government sought to compel Apple to engage in the production of computer code -- code that may incorporate expressive elements -- it is not clear that the government in this case was compelling Apple to engage in protected expression, nor that the Government Order was a content-based or a viewpoint-based regulation of or compulsion of speech. First, as the *Corley* court makes clear, although a government regulation

[67] *Id.* at 61.
[68] *Id.* at 62.
[69] *Id*. at 64.

of computer code *may* target such computer code because of its content, it may also target such computer code based on its functionality and without reference to its content. Although the Apple/FBI case involved the compelled *production* of computer code instead of the *regulation* of computer code, the same principles apply. In the Apple case, as in the *Corley* case, the government was not "concerned with whatever capacity [the source code at issue] might have for conveying information to a human being, and *that capacity . . . is what arguably creates a speech component*…." [70] Rather, the Government Order in this case, like the government regulation at issue in the *Corley* case, compelled the creation of computer code "solely because of its capacity to instruct a [device] to decrypt. *That functional capability is not speech within the meaning of the First Amendment*."[71] Because the Order at issue in this case, like the regulation at issue in the *Corley* case, targeted computer code solely because of its functional capability "without reference to the content of the regulated speech,"[72] the Order at issue here – like the regulation at issue in the *Corley* case – should be analyzed by the court as a content-neutral regulation with an incidental effect on speech (and therefore subject to, at most, intermediate scrutiny under the First Amendment).

Accordingly, the Government Order compelling Apple to produce computer code that performs certain specific functions should not be considered tantamount to a content-based (much less a viewpoint-based) compulsion of expression within the meaning of the Supreme Court's compelled speech jurisprudence. To return to the *Corley* court's skeleton key analogy involving the dual (functional and expressive) nature of computer code, the Government Order in this case is most appropriately analogized to an order compelling a locksmith the produce a key

[70] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (emphasis added).
[71] *Id.* at 454 (emphasis added).
[72] *Id.*

that unlocks a particular set of locks. Despite the fact that the key (like the computer code) may have a slogan printed on it (like the computer code may embody expressive elements), the court should not subject the Order to the strict scrutiny applicable to content-based or viewpoint-based restrictions on -- or compulsions of -- expression. At most, the court should subject the Government's Order to the intermediate scrutiny applicable to content-neutral regulations that have incidental effects on expression as set forth in *Turner Broadcasting Systems v. Federal Communications Commission*,[73] and should consider whether the Order serves as substantial government interest that is unrelated to the suppression of free expression and whether the incidental restriction on speech burdens more speech than necessary to further that interest. In applying this test, the court should hold that the government interest in this case – to secure potential evidence related to a terrorist attack – like the government interest in the *Corley* case, is substantial and that the means used by the government – compelling Apple to produce source code to enable the government to access such potential evidence -- while financially burdensome to Apple, does not substantially burden Apple's free speech rights, and as such, does not burden substantially more speech than is necessary to further that interest.

In short, the syllogism underlying Apple's compelled speech argument is flawed: Although the Government Order compeled the production of computer code, and although computer code may constitute speech protected by the First Amendment, the Government Order does not unconstitutionally compel speech within the meaning of the Supreme Court's compelled speech jurisprudence.

[73] 512 U.S. 622, 662 (1994).