UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203

Case No: 5:16-cm-00010 (SP)

[~~PROPOSED~~] ORDER GRANTING THE MEDIA INSTITUTE'S EX PARTE APPLICATION TO FILE AMICUS CURIAE BRIEF

Hearing Date: March 22, 2016
Hearing Time: 1:00 p.m.
Location: Courtroom 3 or 4.
Judge: Hon. Sheri Pym

IT IS HEREBY ORDERED THAT The Media Institute's Application for *Amicus* Status is GRANTED. The Court grants The Media Institute's *amicus* status.

IT IS FURTHER ORDERED that The Media Institute's amicus curiae proposed brief lodged with this Court on March 3, 2016 is deemed filed as of the date of this Order.

-

Dated this 3rd day of March, 2016

The Honorable Sheri Pym
United States Magistrate Judge

DANIEL SHALLMAN (Bar No. 180782)
Email: dshallman@cov.com
COVINGTON & BURLING LLP
2029 Century Park East, Suite 3100
Los Angeles, California 90067-3044
Telephone: + 1 (424) 332-4752
Facsimile: + 1 (202) 662-6291

KURT WIMMER*
Email: kwimmer@cov.com
LAUREN WILLARD*
Email: lwillard@cov.com
COVINGTON & BURLING LLP
850 10th Street, N.W.
Washington, D.C. 20001
Telephone: + 1 (202) 662-5278
Facsimile: + 1 (202) 662-6291
**Pro hac vice* motion forthcoming

Counsel for Amicus Curiae The Media Institute

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	Case No: 5-16-cm-00010 SP **BRIEF *AMICUS CURIAE* OF THE MEDIA INSTITUTE IN SUPPORT OF APPLE INC.** **Hearing:** Date: March 22, 2016 Time: 1:00 p.m. Location: Courtroom 3 or 4 Judge: Hon. Sheri Pym

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF *AMICUS CURIAE*

Amicus curiae The Media Institute is a nonprofit research foundation specializing in communications policy issues, with a particular emphasis on freedom of speech, a competitive media and communications industry, and excellence in journalism. Founded in 1979, The Media Institute publishes books, prepares regulatory filings and court briefs, and convenes conferences and programs for journalists and communications executives. The Media Institute is one of the leading think tanks focusing on the First Amendment and communications policy.

Dual constitutional cases fought in the 1970s—over compelled speech on the pages of a newspaper and protection for reporter-source confidences—put the U.S. news media on the front lines of the issues raised in this case. *See Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241, 258 (1974) (striking down Florida's "right to reply" statute on the grounds that it violates the First Amendment); *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972) (finding that reporters are obligated to respond to grand jury subpoenas because the compulsion involves "no intrusions upon speech or assembly, no prior restraint or restriction on what the press may publish, and no express or implied command that the press publish what it prefers to withhold"). These issues remain vital industry concerns at a time of stepped-up government leaks investigations and prosecutorial tactics that have included the online impersonation of a prominent national news organization. As journalism has evolved, new digital tools and platforms have become essential means for newsgathering and the dissemination of information to the public. That these constitutional questions are now converging around a mobile device and a technology company does not make them any less critical constitutionally or to the interests of a free press and an informed public.

As an organization representing these interests, The Media Institute is concerned that judicial acceptance of the FBI's assertion that the All Writs Act is a sweeping "residual source of authority" to compel compliance could be construed to

authorize prosecutors with access to digital accounts and devices used by journalists to conscript third parties into efforts to compromise those accounts and devices, without any constitutional limitations. The Media Institute also writes to emphasize that when the government seeks to compel private actors to speak within the meaning of the First Amendment, as it seeks to do with Apple, it must satisfy strict scrutiny to ensure that constitutional rights are adequately protected. For a host of historical and contemporary reasons, the media industry and news organizations are deeply invested in the outcome of this case.

I. INTRODUCTION

This case presents a fundamental question about the government's authority to lawfully require a private actor to speak consistent with the First Amendment. Apple Inc. ("Apple") challenges an order issued under the All Writs Act, 28 U.S.C. § 1651, that compels it to write code that would enable the Federal Bureau of Investigation ("FBI") to access the contents of an iPhone that belongs to San Bernardino County—code Apple asserts is fatal to key security features undergirding its product and, consequently, to the expectations of its users.

The authority on which the FBI relies, the All Writs Act, was enacted by the First Congress in 1789, codified in 1911 and last substantively amended in 1948 to provide: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." Act of June 25, 1948, ch. 646, 62 Stat. 944 (codified as amended at 28 U.S.C. § 1651 (2014)). The All Writs Act "is not a grant of plenary power to the federal courts," *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979), and "does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Penn. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985). The All Writs Act provides courts with a narrow interstitial authority; it does

not authorize the court to issue orders that are addressed or prohibited by other federal statutes or that would interfere with constitutionally protected rights. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, No. 15-1902, 2016 WL 783565, *9 (E.D.N.Y. Feb. 29, 2016) ("*In re Apple*").

Interpreting the All Writs Act to authorize orders such the one issued in this case would raise significant First Amendment concerns and implications for the media industry and the public it serves.

First, reporters rely on secure communications technologies to protect the identities of confidential sources and secure sensitive work product and documentary materials—essential features of constitutionally protected newsgathering. An expanded view of the All Writs Act that would require technology companies to routinely facilitate government access to mobile devices would endanger the media's increasing reliance on mobile technology and devices. The Media Institute recognizes that the current Order does not apply to a company involved in newsgathering. But if the Order becomes a precedent, future orders under the All Writs Act will be sought to be applied against media companies as government authorities seek to acquire access to confidential information stored on mobile devices used by journalists. In light of multiple efforts to obtain information about journalists' newsgathering activities in the context of government investigations, including confidential source identities and confidential materials, the Order's expansive interpretation of the All Writs Act constitutes a danger to journalists' ability to rely on technologies that have become indispensable to modern newsgathering.

Second, by requiring Apple to create new code and sign it cryptographically, the Order seeks to compel Apple to speak within the meaning of the First Amendment. When government seeks to compel a private actor to speak, a reviewing court must apply exacting scrutiny to ensure that First Amendment rights

are adequately protected. Because a lesser standard of scrutiny could undermine constitutional protections for compelled speech in other digital contexts, this Court should apply strict scrutiny to the government's effort to command compliance with the Order at issue here.

For these reasons, the Media Institute respectfully urges this Court to grant Apple's pending motion to vacate the Order as it fails to apply the appropriate constitutional scrutiny. In the alternative, the Media Institute urges the Court to vacate the Order by adopting an interpretation of the All Writs Act that avoids the significant First Amendment concerns at stake.

II. ARGUMENT

A. The Order Undermines the Interests of the News Media in Protecting its Autonomy in Government Investigations and in Maintaining Confidential Communications.

The FBI's reliance on the All Writs Act in this case pays insufficient heed to the necessity of scrutinizing government requests for assistance that implicate First Amendment rights. Because journalists frequently are called upon to assist in criminal investigations, it is of the utmost importance that mechanisms used to compel disclosure and assistance adequately protect the independence of the press. At the same time, orders that jeopardize the confidentiality of communications—including reporter-source confidences—implicate the security of essential newsgathering activities.

1. The Authority the FBI Seeks Under the All Writs Act Would Place the Independence of the Press at Risk.

News and media organizations often possess information—both physical and digital—of interest to law enforcement. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978) (upholding a newsroom search for evidence related to a "violent clash" between demonstrators and police). Under certain circumstances, news organizations may—either voluntarily or after receiving lawful process—produce

information related to criminal investigations to government. For example, when Wichita police were investigating the BTK serial killer in 2004, the *Wichita Eagle* was at the center of the investigation: the newspaper produced letters to the police that it had received from the killer, agreed not to publish certain details from the letter in light of the pending investigation, and held its story from publication for several days upon the request of the police. Matt Thompson, *When the Killer Came Back*, Poynter (Apr. 19, 2004), www.poynter.org/2004/when-the-killer-came-back/22120.

In addition, the government, with some frequency and across administrations led by both parties, seeks to compel reporters and news organizations to disclose information about stories and sources. For example, the government sought testimony from journalists Judith Miller and Matthew Cooper, imprisoning Ms. Miller for contempt. *See In re Grand Jury Subpoena, Judith Miller,* 397 F.3d 964 (D.C. Cir.), *cert. denied,* 545 U.S. 1150 (2005). From 1991 to 2001, the Department of Justice reported issuing 88 subpoena requests in criminal matters, 17 of which "sought information that could lead to the identification of a reporter's source or implicated source material." Daniel J. Bryant, Ltr. to Sen. Charles E. Grassley (Nov. 28, 2001), https://www.rcfp.org/news/documents/grassley.pdf. More recently, the Department of Justice waged a years-long battle to compel New York Times reporter James Risen to testify about his source for a chapter of his book *State of War* even after Risen testified about the damaging effect testifying would have.[1] In June 2013, the public learned that the FBI had identified Fox News journalist James Rosen as a "co-conspirator" in a search warrant application so that it could obtain his e-mails relating to the criminal investigation of a source. *See* Application for Search Warrant

---

[1] Risen testified that "numerous sources of confidential information have told me that they are comfortable speaking to me in confidence specifically because I have shown that I will honor my word and maintain their confidence even in the face of Government efforts to force me to reveal their identities or information." First Motion to Quash Subpoena, Attachment #2, Affidavit of James Risen at ¶ 64, *United States v. Sterling*, 818 F. Supp. 2d 945 (E.D. Va. 2011) (No. 10-485).

for E-mail Account [redacted]@gmail.com, No. 1:10-mj-00291-AK (D.D.C. unsealed Nov. 7, 2011). In December 2014, the United States Attorney for the Southern District of New York sought to compel a producer for CBS "60 Minutes" to testify at a terrorism trial. Tim Cushing, *DOJ Issues First Annual Media Subpoena Report*, TechDirt, (Aug. 20, 2015), https://www.techdirt.com/articles/20150820/07283832013/doj-issues-first-annual-media-subpoena-report.shtml. [2]

More directly, the government has exploited the identity of a major news organization to facilitate an investigation. In 2014, the public learned that the FBI had "impersonated The Associated Press in order to deliver malware to a criminal suspect in the course of an investigation and thereby trace his location." Reporters Comm. for Freedom of the Press, Ltr. to Attorney General Holder and Director Comey (Nov. 6, 2014), *available at* http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf. The 2007 case involved an anonymous suspect in a number of bomb threats to a Seattle area high school. Mike Carter, *FBI created fake Seattle Times Web page to nab bomb-threat suspect*, Seattle Times (Oct. 27, 2014), www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab-bomb-threat-suspect. According to Director Comey, "[r]elying on an agency

---

[2] Indeed, in recognition that law enforcement tools such as subpoenas and warrants "might unreasonably impair newsgathering activities," the Department of Justice has promulgated regulations that require protections prior to issuing subpoenas to the news media. 28 C.F.R. § 50.10; *see also* Dep't of Justice, *Use of Certain Law Enforcement Tools to Obtain Information From, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media* (2015), *available at* http://1.usa.gov/1SaNytG (publishing 2014 data regarding use of law enforcement tools to obtain information from the media); RonNell Andersen Jones, *Avalanche or Undue Alarm? An Empirical Study of Subpoenas Received by the News Media*, 93 Minn. L. Rev. 101, 142 (2008) ("The 761 responding news organizations participating in the study reported that their 'reporters, editors or other news employees' received a total of 3062 'subpoenas seeking information or material relating to newsgathering' in calendar year 2006.").

behavioral assessment that the anonymous suspect was a narcissist, the online undercover officer portrayed himself as an employee of The Associated Press, and asked if the suspect would be willing to review a draft article about the threats and attacks, to be sure that the anonymous suspect was portrayed fairly." James B. Comey, *To Catch a Crook: The F.B.I.'s Use of Deception*, N.Y. Times (Nov. 6, 2014), www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html. When the suspect clicked the link the undercover agent had sent, a "Computer and Internet Protocol Address Verifier" was installed on his machine, his location was revealed, and the suspect was identified. *Id.*

The FBI's conduct in the Seattle matter raised new concerns about the FBI's willingness to harness the news media to serve the agency's investigative ends. The Apple case now creates the haunting scenario of the government seeking to use the All Writs Act to force a news organization to participate directly in an investigation by compelling protected expression without any First Amendment scrutiny. Could the government, armed with a valid warrant, require the Associated Press to write a fictitious article and deploy malicious code on part of its site in order to infect the Seattle suspect's machine and unmask him? *See, e.g.*, *Internet Explorer Zero-Day Used in Watering Hole Attack: Q&A*, Symantec (Dec. 31, 2012), www.symantec.com/connect/blogs/internet-explorer-zero-day-used-watering-hole-attack-qa. Likewise, could it seek an All Writs Act order compelling *The New Yorker*, *The Washington Post*, or any other news organization that has installed SecureDrop to alter its instance to reveal the identity of an anonymous source? *See* SecureDrop, *The Washington Post*, https://www.washingtonpost.com/securedrop/; *see also* SecureDrop, The Official SecureDrop Directory, https://securedrop.org/directory.[3] Surely, conscripting news organizations for

[3] "SecureDrop" is an open-source software system for the anonymous submission of electronic documents originally authored by Aaron Swartz and now managed by the Freedom of the Press Foundation. It is meant to replicate in the digital world the

investigative reasons and forcing them to speak in violation of the First Amendment and their time-honored independence is precisely the sort of "unreasonable burden[]" that "may not be imposed" under the All Writs Act. *United States v. New York Tel. Co.*, 434 U.S. 159, 172 (1977).

Although members of the news media can and do voluntarily assist the government in investigations in certain circumstances, law enforcement is not "free to annex the news media as an investigative arm of government." *Branzburg v. Ohio*, 408 U.S. at 709 (Powell, J., concurring) (internal quotation marks omitted). But if prosecutors may use the All Writs Act unencumbered by First Amendment limitations to compel a private actor to speak in order to effectuate its investigative aims, as the Order at issue does, such an annexation is within the government's reach. Because the government's logic would take it far beyond the case at bar, the Media Institute is concerned that unless the Order is vacated the autonomy of the news media is at risk.

2. Secure Communications Technology Enables Reporters to Engage in Constitutionally Protected Newsgathering.

The Order at issue in this case is also concerning to news and media organizations because it threatens to undermine journalists' trust in the security of tools that they rely upon to gather and produce the news. Reporters use a variety of services to ensure that their communications, contacts, work product, and documentary materials remain confidential. Compelling Apple to create code that undermines the security of its own operating system swings open the door for the FBI

---

familiar phenomenon of documents being left anonymously with a news outlet. *See Bartnicki v. Vopper*, 532 U.S. 514, 519 (2001) (tape "found in . . . mailbox"). A SecureDrop implementation begins with software that can be customized by each news outlet and integrated into its website. It generally permits users who use the Tor browser and correctly follow its procedures to leave electronic documents for recipients in an anonymous manner. *See SecureDrop: A Project of the Freedom of the Press Foundation*, https://securedrop.org/faq.

to compel other service providers to do the same. And when the security of essential tools is compromised, journalists cannot trust the integrity of the platforms that have become essential to the profession.

As the Supreme Court has recognized in a string of recent rulings, communications technology can be crucial to the exercise of free expression and association. Cell phones, in particular, have become in Justice Kennedy's words "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). And, as Justice Sotomayor observed in *Jones*: "Awareness that the Government may be watching chills associational and expressive freedoms." *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

Cell phones also are crucial newsgathering tools. Journalists use cell phones to send and answer email to and from sources and editors, write pitches, stories and articles, record interviews, conduct research, and to accomplish many of the other everyday tasks inherent in the newsgathering process. As Chief Justice Roberts has recognized in the latest of these rulings on communications technologies, cell phones now also serve as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"—all tools that are integral to the journalistic profession. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

Reporters' need for information security tools is closely tied to the core journalistic practice of safeguarding the identities of confidential sources. *The New York Times* used confidential sources to report that the National Security Agency had an illegal wiretapping program that monitored phone calls and e-mail messages involving suspected terrorist operatives without the approval of federal courts. *See* James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), http://nyti.ms/neIMIB. The *Times* also used confidential

sources to report on the harsh interrogations that terrorism suspects in U.S. custody have faced. *See, e.g.*, Scott Shane, David Johnston, and James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), http://nyti.ms/1dkyMgF. *The Washington Post* relied on confidential government sources, among others, to break the story of the Central Intelligence Agency's use of "black sites," a network of secret prisons for terrorism suspects. *See* Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post (Nov. 2, 2005), http://wapo.st/Ud8UD.

When reporters' records are acquired by law enforcement, without adequate safeguards, in order to unmask anonymous sources, the newsgathering process as a whole is harmed. In 2013, the Associated Press learned that the Justice Department had subpoenaed records from twenty Associated Press telephone lines. *See* Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, Associated Press (May 14, 2013), http://bit.ly/11zhUOg. These records, from phone lines used by more than 100 AP reporters and editors, contained metadata—i.e. the numbers, timing, and duration of calls. *See id.*

When this subpoena was revealed, AP President and CEO Gary Pruitt said that the revelation made sources less willing to talk to reporters at his news outlet: "Some of our longtime trusted sources have become nervous and anxious about talking to us, even on stories that aren't about national security." Jeff Zalesin, *AP Chief Points to Chilling Effect After Justice Investigation*, The Reporters Comm. for Freedom of the Press (June 19, 2013), http://rcfp.org/x?CSPl. The chilling effect, Pruitt said, is not limited to the AP: "Journalists at other news organizations have personally told me it has intimidated sources from speaking to them." *Id.*

Because reporters have a constitutional interest in safeguarding their communications, journalism organizations have produced numerous guides on information security. *See, e.g.*, Frank Smyth, Tom Lowenthal and Danny O'Brien, *Journalist Security Guide* Ch. 3, Comm. to Protect Journalists (2012),

https://cpj.org/security/guide.pdf; Silkie Carlo and Arjen Kamphuis, *Information Security for Journalists*, The Centre for Investigative Journalism (July 2015), http://www.tcij.org/resources/handbooks/infosec; Susan McGregor, *Digital Security and Source Protection for Journalists*, Tow Center for Digital Journalism, Columbia Journalism School (July 2014), http://towcenter.org/digital-security-and-source-protection-for-journalists-research-by-susan-mcgregor. These "guides to best computer security practices for journalists," which are often geared toward reporters working in hostile overseas environments confronted by foreign governments and organizations intent on surveilling them at every turn, typically recommend the use of encrypted web browsing tools such as Tor, email encryption protocols like PGP, and encrypted chat clients. *See* Susan E. McGregor *et al.*, *Investigating the Computer Security Practices and Needs of Journalists*, 24th USENIX Security Symposium (Aug. 2015), http://www.franziroesner.com/pdf/journalism-sec15.pdf.

With trust in the security of communications technology so crucial to newsgathering and reporting, it is essential that appropriate safeguards are in place whenever the government seeks to undermine that security. The precedent that emerges from this case will impact the news media as users of technology products and will endanger the media's independence and its crucial role in informing the American public. As a result, this Court should not permit the government to obtain the relief it seeks without ensuring that its request is narrowly tailored to meet a compelling interest.

B. The First Amendment Requires the Government to Satisfy Strict Scrutiny Before Compelling Apple to Speak.

The Supreme Court has long recognized that the First Amendment protects both the freedom to speak and the freedom not to speak. "The right to speak and the right to refrain from speaking are complementary components of the broader concept of 'individual freedom of mind.'" *Wooley v. Maynard*, 430 U.S. 705, 714-15 (1977). The difference between compelled speech and compelled silence "is without

constitutional significance, for the First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what *not* to say." *Riley v. National Federation of the Blind of North Carolina, Inc.*, 487 U.S. 781, 796–97 (1987). Therefore, government actions that "compel speakers to utter or distribute speech bearing a particular message are subject to the same rigorous scrutiny" as laws restricting speech on the basis of their content. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994).

The Order in this case compels Apple, a private actor, to speak within the meaning of the First Amendment. The FBI seeks to require Apple and its engineers to "write[] and cryptographically sign[]" software code. Gov't Motion to Compel Apple Inc. to Comply With This Court's February 16, 2016 Order Compelling Assistance in Search, D.I. 1, at 14. The FBI acknowledges that Apple will be required to "create code that may not now exist." *Id.* at 13. Requiring Apple to design and create computer code to achieve a particular objective compels Apple to engage in expression protected by the First Amendment. In particular, forcing Apple to digitally sign its code compels Apple to express, contrary to its own views, an affirmation that the code is genuine, supported by Apple, and safe to run.

The recognition that this case involves compelled private speech is vital because it requires this Court to apply exacting scrutiny to the FBI's proposed conduct. Compelled speech is a "content-based regulation of speech" subject to strict scrutiny. *Riley*, 487 U.S. at 795. When the government compels someone to "utter or distribute speech bearing a particular message," the government's action must be narrowly tailored to meet a compelling state interest. *Turner Broad. Sys., Inc.*, 512 U.S. at 642.

The careful application of strict scrutiny here is of utmost importance to preserve the guarantee of freedom of speech that underlies the media's ability to serve the public. To hold that the protections of the First Amendment do not apply where the government seeks assistance—in the form of compelled or restrained

speech—because that assistance benefits law enforcement needs would significantly undermine the rights guaranteed by the Constitution.

1. Code is Speech Protected by the First Amendment

The FBI has asked Apple to "build for the FBI a version of Apple's iPhone operating system that does not currently exist" to be loaded onto the phone that, once activated, will disable security features that are potentially active on the device. Decl. of Erik Neuenschwander ISO Mot. to Vacate, D.I. 16-33, ¶ 15. According to Apple, it may do so by either "writ[ing] the tool to submit passcodes electronically" or by creat[ing] a "protocol" that the government can use to accomplish the same ends. *Id.* at ¶ 22. In essence, this Court's order requires Apple to write computer code to disable security features to enable the FBI to effectuate the search warrant.

Federal courts have consistently held that computer code such as that at issue here is speech that "merits First Amendment protection." *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1099 (N.D. Cal. 2004); *see also Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 327 (S.D.N.Y.), *judgment entered*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), 111 F. Supp. 2d at 327 ("As computer code—whether source or object—is a means of expressing ideas, the First Amendment must be considered before its dissemination may be prohibited or regulated.").

Courts also have recognized that code that expresses "cryptographic ideas and algorithms" is expressive for First Amendment purposes. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1140–41 (9th Cir.) *reh'g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999). Indeed, "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code." *Corley*, 273 F.3d at 445. Courts have held that there is "no meaningful difference between computer language . . . and German or French . . . . Like music

and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it." *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996). The Supreme Court has also recognized that the First Amendment applies equally to new forms of technology. *Brown v. Entm't Merchs. Ass'n,* 131 S. Ct. 2729, 2733 (2011) ("[W]hatever the challenges of applying the Constitution to ever-advancing technology, the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary when a new and different medium for communication appears.") (internal citation and quotation marks omitted).

The content of the file requested by the FBI has "both an expressive feature and a functional feature." *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000).[4] Whether Apple builds and delivers ready-to-use software or a protocol for the FBI to use, the Order compels it to create code that is both functional and expressive, and therefore deserving of constitutional protection. What makes the Order even more problematic as a constitutional matter is that for the software update to be accepted on the iPhone, Apple must certify that the software is legitimate. As one commentator noted, "Apple would be being forced to lie to the phone (and by extension its user) . . . notwithstanding the relationship of trust between Apple and its customers on which the security of our digital age depends." Neil Richards, *Apple's "Code=Speech" Mistake*, MIT Technology Review (March 1, 2016), https://www.technologyreview.com/s/600916/apples-code-speech-mistake.[5]

---

[4] Even if the source code requested by the FBI "is essentially functional, that does not remove it from the realm of speech." *Bernstein*, 922 F. Supp. at 1435 ("Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction are often purely functional; they are also speech") (internal citation omitted).

[5] Although the author disagrees with the general argument that code is speech, he agrees that the type of computer code compelled here would violate the First Amendment.

The need to protect functional and expressive code under the First Amendment is made more clear by the manner in which code is used to gather, produce and present news and information to the public. As computer-assisted reporting, computational journalism, and data science—all of which rely on code—gain traction as investigative methods at the core of modern journalism, First Amendment protection for these key newsgathering and publishing tools will only grow more important. *See* Susan McGregor, *CAR hits the mainstream*, Colum. J. Rev. (Mar. 18, 2013), www.cjr.org/data_points/computer_assisted_reporting.php (discussing the importance of machine learning and "algorithmic document analysis" for investigative reporting).

For example, journalists from *The New York Times* and *The Associated Press* are writing code to "create the first free, comprehensive, standardized, linked set of election data for the United States, including federal and statewide offices." OpenElections, *Welcome to OpenElections*, https://blog.openelections.net/19-2. Investigative Reporters and Editors, a nonprofit membership organization, spearheads a Census project "designed to provide journalists with a simpler way to access 2010 Census data so they can spend less time importing and managing the data and more time exploring and reporting the data." Investigative Reporters and Editors, *Home*, census.ire.org. And numerous news organizations write code during the newsgathering and reporting process to facilitate investigative journalism and to create interactive, visual designs for news stories.[6]

---

[6] Examples of the dynamic journalism made possible by newsroom coding projects include Hannah Fairfield, Derek Watkins, and Derek Willis, *Few Women on Some Senate Committees*, N.Y. Times (June 2, 2013), http://www.nytimes.com/interactive/2013/06/03/us/politics/women-on-senate-committees.html; and Sally Kestin and John Maines, *Cops among Florida's worst speeders, Sun Sentinel investigation finds*, Sun Sentinel (Feb. 11, 2012), http://www.sun-sentinel.com/news/speeding-cops/fl-speeding-cops-20120211-story.html.

The importance of code to newsgathering and journalism illustrates what courts have long recognized: code can be both functional and expressive. As a result, "it cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine." *Reimerdes*, 111 F. Supp. at 326.

2. Because the Order Compels Speech, the Government Must Satisfy Strict Scrutiny.

Holding that computer code is speech satisfies a threshold First Amendment question, but not all computer code is therefore impervious to government regulation. Computer code that is fraudulent, incites violence, or facilitates criminal conduct, for example, will not be entitled to heightened protection under the First Amendment. *See United States v. Alvarez*, 132 S. Ct. 2537, 2544 (2012) (listing exceptions to First Amendment heightened protection against content-based regulations). Content-neutral regulations that incidentally affect the ability of a technology company to write computer code also may be permissible under a lower standard of scrutiny. *See Turner Broad. Sys.*, 512 U.S. at 642 ("regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny").

This case, however, involves *compelled* speech. Because computer code is speech, requiring Apple to create code—and attach its signature cryptographically—is compelling Apple to speak within the meaning of the First Amendment. By forcing Apple to create speech that it would otherwise not make and with which it disagrees, the Order falls squarely within the jurisprudence of compelled speech and requires the FBI to satisfy "the most exacting scrutiny." *Id.*

In *Wooley v. Maynard*, a seminal compelled speech case, the Supreme Court held that forcing an individual to display a communication ("Live Free or Die") on his private property (the individual's license plate) violated the First Amendment. 430 U.S. at 717. A person's "individual freedom of mind," the Court reasoned, protects his "First Amendment right to avoid becoming the courier" for the dissemination of speech that he does not wish to communicate. *Id.* at 714, 717. The

reasoning of *Wooley* extends equally, if not more forcefully, to situations where, as here, the government seeks to force an unwilling speaker to *create* the disfavored speech rather than just passively convey someone else's expression.

Another key compelled speech case arose in the context of the news media. In *Miami Herald Publishing Co. v. Tornillo*, the Supreme Court held it unconstitutional to require newspapers to publish the replies of political candidates whom they criticized. 418 U.S. at 258. The Court reasoned that "any such compulsion to publish that which reason tells [a newspaper] should not be published is unconstitutional." *Id.* at 256 (internal quotation marks omitted). Even if the newspaper would face no additional costs and would not forego communication of its own material, the Court held that the compulsory publication requirement would impermissibly interfere with the newspaper's First Amendment right to decide what to print. The precedent in *Tornillo* logically extends to other forms of protected expression, including software code.[7]

The First Amendment does not distinguish between compelled statements of opinion and compelled statements of fact; "either form of compulsion burdens protected speech." *Riley*, 481 U.S. at 797-98. And compelled speech implicates one's rights under the First Amendment regardless of whether the speech involves an ideological message. In *Frudden v. Pilling*, 742 F.3d 1199 (9th Cir. 2014), the Ninth Circuit held that it did not believe that "the First Amendment analysis turns on an examination of the ideological message (or lack thereof)" of the compelled speech. In agreement with the D.C. Circuit, the court held that the right against compelled speech "is not, and cannot be, restricted to ideological messages." *Id.* at 1206 (quoting *Nat'l Ass'n of Mfrs. v. NLRB*, 717 F.3d 947, 957 (D.C. Cir. 2013)). *See also*

---

[7] *See also* Eugene Volokh and Donald M. Falk, *First Amendment Protection for Search Engine Search Results*, 6 (Apr. 20, 2012), http://volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf (applying *Tornillo* to the argument that the First Amendment fully protects search engine results).

Cressman v. Thompson, 719 F.3d 1139, 1152 (10th Cir. 2013) ("[T]he Supreme Court's case law suggests that ideological speech is not the only form of forbidden compelled speech." (citing cases)).

Nor is it of any constitutional significance that a corporation rather than an individual is compelled to speak. *See Pac. Gas & Elec. Co. v. Pub. Util. Comm'n*, 475 U.S. 1, 16 (1986) (plurality opinion) ("For corporations as for individuals, the choice to speak includes within it the choice of what not to say."); *see also Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 342 (2010) (reaffirming that "First Amendment protection extends to corporations").[8]

Because the Order compels speech, strict scrutiny applies. "[M]andating speech that a speaker would not otherwise make necessarily alters the content of the speech" and is therefore a "content-based" action subject to strict scrutiny. *Riley*, 487 U.S. at 795; *see also Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2228 (2015) ("A law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive."). The government is forcing Apple to write specific code that embraces the FBI's view of the precedence of its law enforcement needs

---

[8] That Apple is a commercial entity does not turn the compelled speech at issue into "commercial speech" subject to a lower standard of scrutiny. Commercial speech is defined by the content of the speech and not by the character of the speaker. *See, e.g.*, *Citizens United*, 558 U.S. at 346 (corporation entitled to heightened First Amendment protections for political speech). Commercial speech has been defined as "speech which does no more than propose a commercial transaction." *Virginia Pharmacy*, 425 U.S. 748, 762 (1976). The computer code that Apple is tasked with writing does not "propose a commercial transaction;" indeed, because the purpose of the requested code and signature is to assist the Government with a law enforcement task, it serves no commercial purpose. Furthermore, the Supreme Court has recently held that to justify content-based commercial speech restrictions, "the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest." *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667–68 (2011).

and to overwrite the company's existing computer code that takes the contrary view.[9] The fact that the government disagrees with how Apple writes its code to safeguard personal privacy does not give the government the ability to demand that Apple alter its protected expression without satisfying the highest constitutional hurdles. *See Hurley v. Irish-Am. Gay Grp. of Boston*, 515 U.S. 557, 581 (1995) ("Disapproval of a private speaker's statement does not legitimatize use of the Commonwealth's power to compel the speaker to alter the message by including one more acceptable to others.").[10]

Although it is clear that the government's proposed order involves compelled speech, this finding does not end the inquiry. Strict scrutiny is not "strict in theory,

---

[9] Because the FBI's order requires Apple to create a particular type of software code, this case is distinguishable from cases where the government's requirement did not "'dictate a specific message,' and did not require any 'specific speech at all.'" *Strickland v. City of Seattle*, No. C08-0454 RSM, 2009 WL 2959870, at *4 (W.D. Wash. Sept. 9, 2009) aff'd, 394 F. App'x 407 (9th Cir. 2010) (quoting *Envtl. Def. Ctr., Inc. v. EPA*, 344 F.3d 832, 849 (9th Cir. 2003)).

[10] One might argue that courts routinely compel speech from witnesses in adversary proceedings, and that the Order is no greater an intrusion into Apple's protected speech than an order for a witness to testify. This comparison fails, however, because the use of the All Writs Act to compel Apple to write and sign software code is an entirely new and novel concept not authorized by Congress and unknown to the common law. Compelling the speech of witnesses in court, in contrast, is a constitutionally and statutorily authorized procedure that predates even the founding of our country. *See, e.g.*, *Jaffee v. Redmond*, 518 U.S. 1, 9 (1996) ("For more than three centuries it has now been recognized as a fundamental maxim that the public ... has a right to every man's evidence."). It is appropriately subject to exceptions, including those stated in the Fifth and First Amendments, and various common-law privileges. But it is a false comparison to equate an order conscripting a software company to write code in the service of the United States with an order to compel the testimony of a witness. When Congress wishes to require technology companies to provide assistance to law enforcement, it knows how to do so. *See* Albert Gidari, *CALEA Limits the All Writs Act and Protects the Security of Apple's Phones*, Stanford Center for Internet and Society (Feb. 19, 2016), https://cyberlaw.stanford.edu/blog/2016/02/ calea-limits-all-writs-act-and-protects-security-apples-phones. It has not done so here.

but fatal in fact." *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200, 202 (1995). There may be cases where the government could indeed compel a company to write software. But where, as here, the government compels speech against the speaker's wishes, the court must carefully apply the appropriate level of scrutiny to determine whether the infringement of the speaker's First Amendment rights is justified. Invoking the interests of law enforcement or national security may be relevant to the state's "compelling interest," but the First Amendment requires the government to show a specific interest. It also must demonstrate that any intrusion is being undertaken in a narrowly tailored fashion. Here, serious doubts exist as to whether the government has met its burden to show that it had no other means to achieve its ultimate objective. It is also not clear how critical the information sought is to the government's investigation or that prosecutors could not have used less restrictive means in seeking Apple's compliance.

This case elevates long recognized protections fundamental to both the public and the press to the digital platforms of the Internet era. This Court cannot disregard potential infringements on First Amendment rights merely because the government needs assistance in a criminal or national security investigation.[11] Permitting the government to compel a private party to write software or publish information whenever it offers a law enforcement justification without engaging in exacting First Amendment scrutiny will set a dangerous precedent and may invite future and more troubling incursions on the freedom of speech.

C. Under the Constitutional Avoidance Canon, the Court Should Interpret the All Writs Act Not to Permit the Order.

Even if it is a close question whether the government's proposed order would violate Apple's First Amendment rights, the significant risk of a constitutional

---

[11] Of course, the government may ask individuals and companies to assist in investigations, as Apple has already done. When a person voluntary engages in speech without coercion, no First Amendment concerns are present.

violation should lead this Court to reject the FBI's proposed interpretation of the All Writs Act. Under the canon of constitutional avoidance, "if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' [a court is] obligated to construe the statute to avoid such problems." *I.N.S. v. St. Cyr*, 533 U.S. 289, 299–300 (2001) (citations omitted). As demonstrated, an interpretation of the All Writs Act to permit the government to compel Apple to write and sign computer code raises substantial First Amendment concerns.

Because the interpretation of the All Writs Act proposed by Apple is equally, if not more, plausible in light of the text of the statute and the relevant case law,[12] the Court should adopt that interpretation and avoid resolving the more difficult constitutional question. Indeed, courts routinely adopt narrowing statutory constructions to avoid striking down statutes that appear to violate the First Amendment. *See, e.g.*, *Lowe v. SEC*, 472 U.S. 181, 210 (1985) (adopting a narrow construction of the Investment Advisors Act of 1940 to exclude the publication of investment newsletters "[a]s long as the communications between petitioners and their subscribers remain entirely impersonal and do not develop into the kind of fiduciary, person-to-person relationships that were discussed at length in the legislative history of the Act."). Likewise, in 2005, the Ninth Circuit concluded that the denial of a request for an injunction to stop labor picketing under the National Labor Relations Act was appropriate because the picketers had made a "colorable" claim that the injunction would violate their First Amendment rights. *See Overstreet v. United Bhd. of Carpenters & Joiners of Am., Local Union No. 1506*, 409 F.3d

---

[12] Indeed, in a decision issued just this week, Magistrate Judge Orenstein of the Eastern District of New York agreed with Apple's interpretation of the All Writs Act holding that the Act does not require Apple to supply similar technical assistance (unlocking an iPhone) to the government. *See In re Apple*, No. 15-1902, 2016 WL 783565 (E.D.N.Y. Feb. 29, 2016).

1199, 1209 (9th Cir. 2005) ("Our need to avoid creating a 'significant risk' to the First Amendment affects both how we proceed to interpret the statute at issue and the degree to which we take into account Overstreet's view of the statute."). This Court should adopt the interpretation of the All Writs Act that avoids the First Amendment concerns implicated when the government seeks to compel Apple to write computer code.

III. CONCLUSION

For the reasons set forth herein, The Media Institute urges this Court to vacate the Order.

Dated: March 3, 2016

Respectfully submitted,

Dan Shallman
N.L.

DANIEL SHALLMAN (Bar No. 180782)
Email: dshallman@cov.com
COVINGTON & BURLING LLP
2029 Century Park East, Suite 3100
Los Angeles, California 90067-3044
Telephone: + 1 (424) 332-4752
Facsimile: + 1 (202) 662-6291

KURT WIMMER*
Email: kwimmer@cov.com
LAUREN WILLARD*
Email: lwillard@cov.com
COVINGTON & BURLING LLP
850 Tenth Street, N.W.
Washington, D.C. 20001-4956
Telephone: + 1 (202) 662-5278
Facsimile: + 1 (202) 662-6291
**Pro Hac Vice* motion forthcoming

Attorneys for *Amicus Curiae*
The Media Institute