Martin J. Mayer, SBN 73890
James R. Touchstone, SBN 184584
Name: Tarquin Preziosi, SBN 198014
Address: Jones & Mayer, 3777 N. Harbor Blvd.
Fullerton, CA 92835
Phone: ((714) 446-1400
Fax: (714) 446-1448
Attorneys for Amici Applicants

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

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 3KGD203	CASE NUMBER: 5:16-cm-00010-SP
	BRIEF OF AMICI CURIAE AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF AMICI CURIAE BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

BRIEF OF AMICI CURIAE

I. STATEMENT OF FACTS AND PROCEDURAL HISTORY.

Amici accept the procedural history and pertinent facts as set forth in the briefs of the United States and Apple. Amici understand that the substantive legal issues that are at stake in this matter will be fully briefed by the United States Attorney's Office. Amici defer to the legal arguments of the United States office on these issues.

II. INTRODUCTION.

This matter stems from the FBI's lawful seizure of an Apple iPhone that was used by Syed Rizwan Farook ("Farook") in carrying out the December 2, 2015 massacre in San Bernardino. Farook, along with his wife, murdered 14 people and injured 22 others. The United States has fully complied with the Fourth Amendment in seizing and attempting to gain access to the contents of the iPhone – both by obtaining a warrant to search the phone and securing consent from the owner of the phone. Nevertheless, Apple retains the exclusive technical ability to access the data from the iPhone and has refused to assist in obtaining the requested access.

In order to protect the American public from a possible future attack, law enforcement needs to be able to use the existing legal tools at their disposal. These tools are the warrant and order compelling compliance therewith.

The legal and privacy issues surrounding this case have been much debated in the media. Apple has stated – both publically and to this court – that granting the United States' motion to compel would compromise the security of personal data on millions of iPhones. In essence, Apple has set up an argument that pits the privacy interests of its user's data against the needs of a government investigation into passed events. This argument is misplaced. The requested order would allow Apple to achieve the goals of unlocking the iPhone in a technical manner of

Apple's choosing. See February 16, 2016 Order Compelling Apple Inc. to Assist Agents in Search, pg. 3, ¶ 4 ("Order"); Memorandum of Points and Authorizes in Support of Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, pg. 4. Thus, Apple can be in exclusive control of the methods to unlock this iPhone. The possible future failure of Apple to safeguard these methods from potential disclosure cannot outweigh the present compelling need of the public to be protected.

Amici of course concur that society does not tolerate violations of the Fourth Amendment - and that is exactly what has *not* occurred here. As tacitly conceded by Apple, the various law enforcement agencies involved followed the letter of the law in seizing and attempting to search this iPhone. Law enforcement is not now asking this Court to compel the "locksmith" to give them a master key to unlock all locks built by this locksmith. Nor is law enforcement asking the locksmith to leave all similar doors unlocked. Rather, the United States is asking the court to compel the locksmith to simply unlock this one door in the manner of the locksmith's choosing. How the locksmith goes about unlocking that door and retaining, securing, and/or discarding the key is up to the locksmith.

III. THE GOVERNMENT HAS FULLY COMPLIED WITH THE FOURTH AMENDMENT AND WILL BE REQUIRED TO DO SO IN ALL FUTURE SEARCHES.

The iPhone at issue is owned by the County of San Bernardino Department of Public Health ("SBCDPH"), which was Farook's employer at the time of the massacre. It was assigned to and used by Farook as part of his employment with SBCDPH. Farook accepted SBCDPH's written policy that all such devices are subject to search by SBCDPH. The iPhone was lawfully seized pursuant to a federal search warrant issued by Magistrate Judge David T. Bristow on December 3, 2015. SBCDPH, as the owner of the

phone, has given consent to the search of the iPhone and to Apple's assistance in the search. As such, even if a warrant had not been obtained, the only entity with cognizable privacy interest in this iPhone has consented to the search. Nevertheless, all requirements of the Fourth Amendment related to the search and seizure of this iPhone have been satisfied.

The Order is limited to this iPhone; it does not, nor can it be applied to items that were not seized pursuant to the warrant in this case. Law enforcement would necessarily have to comply with the Fourth Amendment in any future searches of iPhones by seeking a warrant and/or consent of the owner. Apple's argument that the "government has filed multiple other applications for similar orders" simply proves this point. See Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance, pg. 3. ("Motion to Vacate"). This case does not set the precedent that Apple fears. For example, in a recent ruling from the Eastern District of New York, the court there denied the government's request for an order requiring Apple to bypass the passcode security on an iPhone. [1]

The Order does not compel Apple to turn over the methods it uses for disabling the auto-erase function to the government. Nor does the Order actually compel Apple to keep or otherwise maintain the program that it creates to disable the auto-erase function. Apple would be free to destroy or otherwise discard any code that it creates to comply with this Order. If Apple chooses to retain that program, any potential breach of security would not be attributable to any governmental action.

///

[1] See Memorandum and Order, February 29, 2016, *In re Order Requiring Apple Inc. to Assist in the Execution of Search Warrant Issued by This Court*, E.D.N.Y No. 15-MC-1902 (JO), Doc. 29, at 1. This ruling is limited to the particular circumstances of that case. See id. at 1. There, the iPhone was owned by an individual arrested for methamphetamine trafficking – not the county itself that consented to the search of the phone. See id. at 2. Further, the government waited well over a year after seizing the iPhone to seek the order to compel Apple's assistance. See id. at 2-4. In short, the application of this ruling should be limited to its facts.

Given the cited time and expense to create such a program, it would not be inequitable to require any agency that secured a warrant to be required to compensate Apple for the legitimate expenses incurred in complying with such an order. In short, all of the procedural safeguards of the Fourth Amendment will necessarily remain in place and be applicable to any future cases.

The ultimate decision to mandate that all companies such as Apple be compelled to create a back door to their operating systems is clearly a political, not a judicial, function. However, vacating this Order on that premise while we as a nation await congressional action (or inaction) would be a disservice to the American public. In order to adequately do their job, law enforcement needs to be able to use the existing tools at their disposal to gain access to critical information on a case by case basis. One only needs alter a few facts of the 2010 Times Square car bombing attempt to illustrate this point. Replace the "smoke" that alerted passers-by to the location of the car bomb with "data" on a locked iPhone and the dilemma faced by law enforcement is evident. In that hypothetical situation, where seconds count, what tools does law enforcement have? Absent voluntary compliance by Apple, or its compliance with a court order, law enforcement would be in exactly the same position that it is in now – hampered in its efforts to provide for the public's safety.

Manifestly, Apple is refusing to assist the United States in its attempt to search this iPhone. Part of the reasons for its present position is apparently Apple's opinion that this litigation might not have been necessary if the FBI had consulted with Apple first before an iCloud account password was changed. See Motion to Vacate, pg. 11. This statement is repugnant to California Law Enforcement. Apple is, in essence, saying to the government "you had your chance". Amici respectfully request that this court disregard this argument in its analysis of the public safety issues at stake here.

///

///

This case amply demonstrates that law enforcement has complied with the applicable Fourth Amendment safeguards here, and will be required to do so in all other cases. Apple's argument to the contrary is unsupported. Apple's fears regarding potential future security breaches as a result of this Order is simply speculation. Some possible future invasion of the iPhone security system – attributable solely to third parties who gained access to Apple's code via Apple's failure to secure (or even destroy) this code - does not outweigh the government's present compelling need in this case.

IV. THIS ORDER DOES NOT OFFEND THE FIRST AMENDMENT.

The Order, is, at most, a means to an end: to disable the auto-erase function of this iPhone so that it can be searched without the risk of losing all data. It does not "compel" Apple to engage in protected "speech" in any particular manner. While Amici do not dispute that computer code can be speech, it is certainly not compelled speech in the manner asserted by Apple. See *Riley v. Nat'l Fed'n of Blind* (1988) 487 U.S. 781, 798, 108 S.Ct. 2667, 2678, 101 L.Ed.2d 669, 690 (exacting scrutiny applied to the requirement that professional fundraisers disclose to potential donors, before an appeal for funds, the percentage of charitable contributions collected during the previous 12 months that were actually turned over to charity).

Similarly, the Order cannot legitimately be characterized as impermissible viewpoint discrimination, any more than would a court order compelling compliance with signage standards under the Americans with Disabilities Act.

The realities of what computer code is, and its normal functions, "require a First Amendment analysis that treats code as combining nonspeech and speech elements, *i.e.*, functional and expressive elements." *Universal City Studios v. Corley* (2d Cir. 2001) 273 F.3d 429, 451, citing *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 386, 23 L. Ed. 2d 371, 89 S. Ct. 1794 (1969) ("Differences in the characteristics of new media justify differences in the First Amendment standards applied to them.") Assuming, *arguendo*, that the Order compels "speech" on the part of Apple, the Order is a content neutral

directive to disable a single function of this iPhone – especially since the manner of achieving that end is left to Apple.

Given these realities of "speech" in the context of computer code – and as set forth in the cases cited by Apple - the appropriate standard to be applied is intermediate scrutiny, i.e., if "it furthers an important or substantial governmental interest." *Junger v. Daley* (6th Cir. 2000) 209 F.3d 481, 485, citing *United States v. O'Brien* (1968) 391 U.S. 367, 377, 88 S.Ct. 1673, 1679, 20 L.Ed.2d 672, 680; see *321 Studios v. MGM Studios, Inc.* (N.D.Cal. 2004) 307 F.Supp.2d 1085, 1101 (applying intermediate scrutiny to regulation of computer code); *United States v. Elcom Ltd.* (N.D.Cal. 2002) 203 F.Supp.2d 1111, 1127-1128 (same). Under intermediate scrutiny, the Government must "demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way." *Turner Broadcasting System, Inc. v. FCC* (1994) 512 U.S. 622, 624, 129 L.Ed.2d 497, 114 S.Ct. 2445.

Nevertheless, whether the test is "intermediate", "strict" or "exacting" scrutiny, the standard has been met in this case. This should not be an academic debate about First Amendment protections or, as Apple suggests, one that can only be resolved through the political process. Apple characterizes the need to access the iPhone as speculative; claiming the iPhone was used in a past event where "any criminal activity linked to the phone at issue ended two months ago when the terrorists were killed". See Motion to Vacate, pg. 21. This is myopic and disingenuous.

The massacre of December 2, 2015 – carried out by terrorists who pledged their allegiance to ISIL - is a manifestation of a threat that has not ceased. The United States has clearly set forth the value that data on this iPhone may have in the ongoing efforts to protect the American people. Simply because the Order, might, in some way, compel Apple to write code of its choosing to disable the auto-erase function, cannot, and does not violate the First Amendment here.

V. CONCLUSION.

For all of the foregoing reasons, Amici respectfully request that this Court grant the United States' Application for Order Compelling Apple Inc. to Assist Agents in Search.

Dated: March 3, 2016

Respectfully submitted,

JONES & MAYER

By: */s/ Martin J. Mayer*
Martin J. Mayer
James R. Touchstone
Tarquin Preziosi
Attorneys for Amici Applicants

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF ORANGE

I am employed in the County of Orange, State of California. I am over the age of 18 and not a party to the within action. My business address is 3777 North Harbor Boulevard, Fullerton, California 92835.

On March 3, 2016, I served the within **APPLICATION FOR LEAVE TO FILE AMICI CURIAE BRIEF; STATEMENT OF IDENTITY AND INTEREST OF AMICI CURIAE; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF AMICI CURIAE BRIEF** on the interested parties in said action by placing [X] a true and correct copy or [ ] delivered by one or more of the means set forth below:

SEE ATTACHED SERVICE LIST

[✓] [***Via Mail***] By depositing said envelope with postage thereon fully prepaid in the United States mail at La Habra, California. I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under that practice, it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid at La Habra, California, in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit of mailing in affidavit.

[ ] [***Via Electronic Service***] By electronically transmitting the document(s) listed above to the email address(es) of the person(s) set forth on the attached service list. The transmission was reported as complete and without error. *See* Rules of Court, Rule 2.251.

[✓] [***Federal***] I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made.

Executed on March 3, 2016 at Fullerton, California.

Laura D Miller

LAURA MILLER

SERVICE LIST

Eric David Vandevelde
Gibson Dunn & Crutcher LLP
333 S. Grand Ave.
Los Angeles, CA 90071
evandevelde@gibsondunn.com
Attorney for Respondent Apple Inc.

Nicole T. Hanna
Gibson Dunn and Crutcher LLP
3161 Michelson Drive 12th Floor
Irvine, CA 92612
nhanna@gibsondunn.com
Attorney for Respondent Apple Inc.

Theodore J. Boutrous, Jr.
Gibson Dunn and Crutcher LLP
333 South Grand Ave.
Los Angeles, CA 90071
tboutrous@gibsondunn.com
Attorney for Respondent Appe Inc.

Theodore B. Olson
Gisbosn Dunn and Crutcher
1050 Connecticut Ave N W
Washington DC 20036
TOlson@gibsondunn.com
Attorney for Respondent Apple Inc.

Allen W. Chiu
AUSA – Office of US Attorney
National Security Section
312 N. Spring St., Suite 1300
Los Angeles, CA 90012
allen.chiu@usdoj.gov
Attorney for Plaintiff USA

Tracy L. Wilkison
AUSA Office of US Attorney
Chief, Cyber and Intellectual Property Crimes Section
312 N. Spring St., 11th Floor
Los Angeles, CA 90012
Tracy.wilkison@usdoj.gov
Attorney for Plaintiff USA

PROOF OF SERVICE