EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section
ALLEN W. CHIU (California Bar No. 240516)
Assistant United States Attorney
Terrorism and Export Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0622/2435
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov
Allen.Chiu@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE 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 35KGD203	ED No. CM 16-10 [redacted] (SP) GOVERNMENT'S MOTION TO COMPEL APPLE INC. TO COMPLY WITH THIS COURT'S FEBRUARY 16, 2016 ORDER COMPELLING ASSISTANCE IN SEARCH; EXHIBIT Hearing Date: March 22, 2016 Hearing Time: 1:00 p.m. Location: Courtroom of the Hon. Sheri Pym

The United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, and Assistant United States Attorneys Tracy L. Wilkison and Allen W. Chiu, hereby files its Motion to Compel Apple Inc. ("Apple") to Comply with this Court's February 16, 2016 Order Compelling Apple To Assist Agents In Its Search.

This Motion is based upon the attached memorandum of points and authorities, the attached exhibit, the files and records in this case including the application and order compelling Apple to assist the FBI and the underlying search warrant, and such further evidence and argument as the Court may permit.

Dated: February 19, 2016

Respectfully submitted,

EILEEN M. DECKER
United States Attorney

PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division

TRACY L. WILKISON
ALLEN W. CHIU
Assistant United States Attorneys

Attorneys for Applicant
UNITED STATES OF AMERICA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL STATUTES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Rather than assist the effort to fully investigate a deadly terrorist attack by obeying this Court's Order of February 16, 2016, Apple has responded by publicly repudiating that Order. See Exhibit 1. Apple has attempted to design and market its products to allow technology, rather than the law, to control access to data which has been found by this Court to be warranted for an important investigation. Despite its efforts, Apple nonetheless retains the technical ability to comply with the Order, and so should be required to obey it.

Before Syed Rizwan Farook ("Farook") and his wife Tafsheen Malik shot and killed 14 people and injured 22 others at the Inland Regional Center in San Bernardino, Farook's employer issued him an iPhone. The Federal Bureau of Investigation ("FBI") recovered that iPhone during the investigation into the massacre. The government has reason to believe that Farook used that iPhone to communicate with some of the very people whom he and Malik murdered. The phone may contain critical communications and data prior to and around the time of the shooting that, thus far: (1) has not been accessed; (2) may reside solely on the phone; and (3) cannot be accessed by any other means known to either the government or Apple. The FBI obtained a warrant to search the iPhone, and the owner of the iPhone, Farook's employer, also gave the FBI its consent to the search. Because the iPhone was locked, the government subsequently sought Apple's help in its efforts to execute the lawfully issued search warrant. Apple refused.

Apple left the government with no option other than to apply to this Court for the Order issued on February 16, 2016. The Order requires Apple to assist the FBI with respect to this single iPhone used by Farook by providing the FBI with the opportunity to determine the passcode. The Order does not, as Apple's public statement alleges, require Apple to create or provide a "back door" to every iPhone; it does not provide "hackers and criminals" access to iPhones; it does not require Apple to "hack [its] own users" or to "decrypt" its own phones; it does not give the government "the power to reach into anyone's device" without a warrant or court authorization; and it does not compromise the security of personal information. See Exhibit 1. To the contrary, the Order allows Apple to retain custody of its software at all times, and it gives Apple flexibility in the manner in which it provides assistance. In fact, the software never has to come into the government's custody.

In the past, Apple has consistently complied with a significant number of orders issued pursuant to the All Writs Act to facilitate the execution of search warrants on Apple devices running earlier versions of iOS.[1] The use of the All Writs Act to facilitate a warrant is therefore not unprecedented; Apple itself has recognized it for years. Based on Apple's recent public statement and other statements by Apple, Apple's current refusal to comply with the Court's Order, despite the technical feasibility of doing so, instead

[1] Apple's Legal Process Guidelines continue to state that Apple will provide assistance with unlocking devices running iOS versions earlier than 8.0, and advises as to what language to include in the order. See "Extracting Data from Passcode Locked iOS Devices," Apple Legal Process Guidelines § III(I) (updated September 29, 2015), available at http://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf. However, Apple has informed another court that it now objects to providing such assistance.

appears to be based on its concern for its business model and public brand marketing strategy.[2]

Accordingly, the government now brings this motion to compel. While the Order includes the provision that "to the extent that Apple believes that compliance with this Order would be unreasonably burdensome, it may make an application to this Court for relief within five business days of receipt of the Order," Apple's public statement makes clear that Apple will not comply with the Court's Order. The government does not seek to deny Apple its right to be heard, and expects these issues to be fully briefed before the Court; however, the urgency of this investigation requires this motion now that Apple has made its intention not to comply patently clear.[3] This aspect of the investigation into the December 2, 2015 terrorist attack must move forward.

II. STATEMENT OF FACTS

As set forth in the government's application for the All Writs Act Order, and the Declaration of FBI Supervisory Special Agent ("SSA") Christopher Pluhar, which was attached thereto, both of which were filed on February 16, 2016, the FBI has been investigating the

[2] As Apple has stated on its web page, "Our commitment to customer privacy doesn't stop because of a government information request. … Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS8." (https://web.archive.org/web/20140918023950/http://www.apple.com/privacy/government-informaton-requests/). Notably, notwithstanding this previous statement, Apple concedes that it has retained the ability to do as the Court ordered.

[3] Although a separate order compelling Apple's compliance with this Court's February 16, 2016, order is not legally necessary, in light of Apple's publicly stated "[o]pposing [of] this order" and its stated interest in adversarial testing of the order's legal merits, the government files this noticed motion to provide Apple with the due process and adversarial testing it seeks.

December 2, 2015 mass murder of 14 people, and the shooting and injuring of 22 others, at the Inland Regional Center ("IRC") in San Bernardino, California, and the participation by Farook and his wife Malik in that crime. Farook and Malik died later that day in a shoot-out after a pursuit with law enforcement.

Since that time, the FBI has been tirelessly investigating the precise role of those who may have been involved in the attack. As part of this investigation, the FBI obtained search warrants to search, among other locations and items, the digital devices and online accounts of Farook and Malik. Through those searches, the FBI has discovered crucial information about the attack. For example, the FBI discovered that on December 2, 2015, at approximately 11:14 a.m., a post on a Facebook page associated with Malik stated, "We pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi," referring to Abu Bakr Al Baghdadi, the leader of Islamic State of Iraq and the Levant ("ISIL"), also referred to as the Islamic State ("IS"), or the Islamic State of Iraq and al-sham ("ISIS"), or Daesh. ISIL is designated as a foreign terrorist organization by the United States Department of State and has been so designated since December 2004. Moreover, a search warrant executed at Farook's residence resulted in the discovery of thousands of rounds of ammunition and over a dozen pipe bombs.

In addition, as part of the FBI's investigation, on December 3, 2015, the Honorable David T. Bristow, United States Magistrate Judge, issued a search warrant in Docket Number ED 15-0451M for a black Lexus IS300, which was a vehicle that Farook used. The vehicle was parked outside of his residence where the thousands of rounds of ammunition and pipe bombs were found. The search warrant for the

vehicle also ordered the search of digital devices located within it. Inside the vehicle the FBI found a cellular telephone of an Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network (the "SUBJECT DEVICE"). The SUBJECT DEVICE is owned by Farook's employer at the San Bernardino County Department of Public Health ("SBCDPH"), and was assigned to, and used by, Farook as part of his employment. The SBCDPH provided the government its consent to search the SUBJECT DEVICE and to Apple's assistance with that search.[4]

Nonetheless, despite the search warrant ordered by the Court and the owner's consent to search the SUBJECT DEVICE, the FBI has been unable to search the SUBJECT DEVICE because it is "locked" or secured with a user-determined, numeric passcode. More to the point, the FBI has been unable to make attempts to determine the passcode to access the SUBJECT DEVICE because Apple has written, or "coded," its operating systems with a user-enabled "auto-erase function" that would, if enabled, result in the permanent destruction of the required encryption key material after 10 failed attempts at the entering the correct passcode (meaning that, after 10 failed attempts, the information on the device becomes permanently inaccessible).

The information and data contained on the SUBJECT DEVICE is of particular concern to the government because, while evidence found on the iCloud account associated with the SUBJECT DEVICE indicates that Farook communicated with victims who were later killed during the

---

[4] In addition, SBCDPH has a written policy that all digital devices are subject to search at any time by the SBCDPH, which Farook accepted via signature upon employment.

shootings on December 2, 2015, the backup iCloud data which the government has been able to obtain for the account ends on October 19, 2015. In addition, toll records for the SUBJECT DEVICE establish that Farook communicated with Malik using the SUBJECT DEVICE between July and November 2015, but this information is not found in the backup iCloud data. Accordingly, there may be critical communications and data prior to and around the time of the shooting that thus far has not been accessed, may reside solely on the SUBJECT DEVICE; and cannot be accessed by any other means known to either the government or Apple.

When the government first realized that Apple retained the means to obtain that data from the SUBJECT DEVICE and that due to the way that Apple created the software Apple was the only means of obtaining that data, the government sought Apple's voluntary assistance. Apple rejected the government's request, although it conceded that it had the technical capability to help. As a result, without any other alternative, on February 16, 2016, the government applied for — and this Court subsequently issued — an Order pursuant to the All Writs Act, compelling Apple to assist the FBI in its search of the SUBJECT DEVICE.

After the government served this Court's Order on Apple, Apple issued a public statement responding directly to the Order. See Exhibit 1. In that statement, Apple again did not assert that it lacks the technical capability to execute the Order, that it is not essential to gaining access into the iPhone, or that it would be too time- or labor-intensive. Rather, Apple appears to object based on a combination of: a perceived negative impact on its reputation and marketing strategy were it to provide the ordered assistance to the

government, numerous mischaracterizations of the requirements of the Order, and an incorrect understanding of the All Writs Act.

III. THE COURT SHOULD ISSUE AN ORDER COMPELLING APPLE TO COMPLY WITH ITS ORDER REQUIRING ASSISTANCE WITH THE FBI'S SEARCH OF THE SUBJECT DEVICE PURSUANT TO THE ALL WRITS ACT

A. This Court's All Writs Act Order is Lawful and Binding

To the extent that Apple objects that the Court does not have authority under the All Writs Act to compel Apple to assist in the execution of a lawfully obtained search warrant, this objection fails because the authority to require reasonable third-party assistance that is necessary to execute a warrant is well-established, and no provision of any other law or any judicial decision justifies limitation of that All Writs Act authority. To allow Apple not to comply with the Order would frustrate the execution of a valid warrant and thwart the public interest in a full and complete investigation of a horrific act of terrorism.

1. The All Writs Act

The All Writs Act provides in relevant part that "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." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." Pennsylvania Bureau of Correction v. United States Marshals Service, 474 U.S. 34, 43 (1985). Pursuant to the All Writs Act, the Court has the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers." Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979) (citing United States v. New York Telephone Co., 434 U.S.

159 (1977)). The All Writs Act permits a court, in its "sound judgment," to issue orders necessary "to achieve the rational ends of law" and "the ends of justice entrusted to it." New York Telephone Co., 434 U.S. at 172-73 (citations and internal quotation marks omitted). Courts must apply the All Writs Act "flexibly in conformity with these principles." Id. at 173; accord United States v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012) ("[C]ourts have significant flexibility in exercising their authority under the Act.") (citation omitted).

In New York Telephone Co., the Supreme Court held that courts have authority under the All Writs Act to issue supplemental orders to third parties to facilitate the execution of search warrants. The Court held that "[t]he power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, … and encompasses even those who have not taken any affirmative action to hinder justice." Id. at 174. In particular, the Court upheld an order directing a phone company to assist in executing a pen register search warrant issued under Rule 41. See id. at 171-76; see also In re Application of United States for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities (Mountain Bell), 616 F.2d 1122, 1132-33 (9th Cir. 1980) (affirming district court's order compelling Mountain Bell to trace telephone calls, on grounds that "the obligations imposed . . . were reasonable ones." (citing New York Telephone Co., 434 U.S. at 172)). New York Telephone Co. also held that "Rule 41 is not limited to tangible items but is sufficiently flexible to include within its

scope electronic intrusions authorized upon a finding of probable cause." 434 U.S. at 169. The Court relied upon the authority of a search warrant pursuant to Rule 41 to predicate an All Writs Act order commanding a utility to implement a pen register and trap and trace device - before Congress had passed a law that specifically authorized pen registers by court order. Under New York Telephone Co. and Mountain Bell, the Court had authority pursuant to the All Writs Act to issue the Order.

Further, based on the authority given under the All Writs Act, courts have issued orders, similar to the one the Court issued here, that require a manufacturer to attempt to assist in accessing a cellphone's image files so that a warrant may be executed as originally contemplated. See, e.g., In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone (In re XXX), 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014); see also United States v. Navarro, No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013). Courts have also issued All Writs Act orders in support of warrants in a wide variety of contexts, including ordering a phone company to assist with a trap and trace device (Mountain Bell, 616 F.2d at 1129); ordering a credit card company to produce customer records (United States v. Hall, 583 F. Supp. 717, 722 (E.D. Va. 1984)); ordering a landlord to provide access to security camera videotapes (In re Application of United States for an Order Directing X to Provide Access to Videotapes (Access to Videotapes), 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003)(unpublished)); and ordering a phone company to assist with consensual monitoring of a customer's calls (In re Application of the United States for an Order Directing a Provider of Communication

Services to Provide Technical Assistance to the DEA, 2015 WL 5233551, at *4-5 (D.P.R. Aug. 27, 2015)). The government is also aware of multiple other unpublished orders in this district and across the country compelling Apple to assist in the execution of a search warrant by accessing the data on devices running earlier versions of iOS, orders with which Apple complied.[5] In fact, as noted above, Apple has long recognized this application, and has complied with search warrants compelling Apple to extract data from older iOS devices locked with a passcode. Until last year, Apple did not dispute any such order.

In New York Telephone Co., the Supreme Court considered three factors in concluding that the issuance of the All Writs Act order to the phone company was appropriate. First, it found that the phone company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." Id. at 174. Second, it concluded that the order did not place an undue burden on the phone company. See id. at 175. Third, it determined that the assistance of the company was necessary to achieve the purpose of the warrant. See id. As set forth below, each of these factors supports the order issued in this case.

2. Apple is not "far removed" from this matter

First, Apple is not "so far removed from the underlying controversy that its assistance could not be permissibly compelled."

[5] In litigation pending before a Magistrate Judge in the Eastern District of New York, that court sua sponte raised the issue of whether it had authority under the All Writs Act to issue a similar order. That out-of-district litigation remains pending without any issued orders, nor would any such order be binding on this Court. In any event, that litigation represents a change in Apple's willingness to access iPhones operating prior iOS versions, not a change in Apple's technical ability.

Apple designed, manufactured and sold the SUBJECT DEVICE, and wrote and owns the software that runs the phone – which software is preventing the search for evidence authorized by the warrant. Indeed, Apple has positioned itself to be essential to gaining access to the SUBJECT DEVICE or any other Apple device, and has marketed its products on this basis. See, e.g., Apple's Security Guide, www.apple.com/business/docs/iOS_Security_Guide.pdf. Apple designed and restricts access to the code for the auto-erase function – the function that makes the data on the phone permanently inaccessible after multiple failed passcode attempts. This feature effectively prevents the government from performing the search for evidence authorized by the warrant without Apple's assistance. The same software Apple is uniquely able to modify also controls the delays Apple implemented between failed passcode attempts - which makes the process take too long to enable the access ordered by the Court. Especially but not only because iPhones will only run software cryptographically signed by Apple, and because Apple restricts access to the source code of the software that creates these obstacles, no other party has the ability to assist the government in preventing these features from obstructing the search ordered by the Court pursuant to the warrant. Just because Apple has sold the phone to a customer and that customer has created a passcode does not mean that the close software connection ceases to exist; Apple has designed the phone and software updates so that Apple's continued involvement and connection is required.

Apple is also not made "far removed" by the fact that it is a non-government third party. While New York Telephone Co. and Mountain Bell involved public utilities, limiting All Writs Act

orders to public utilities is inconsistent with the broad scope of judicial authority under the All Writs Act. New York Telephone Co. emphasized that "the Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis[,]" and the company's noncompliance "threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used." 434 U.S. at 174. In Mountain Bell, the Ninth Circuit emphasized that its decision "should not be read to authorize the wholesale imposition upon private, third parties of duties pursuant to search warrants," 616 F.2d at 1132, but Apple is not a random entity summoned off the street to offer assistance, nor is it the target of the investigation. Where Apple designed its software and that design interferes with the execution of search warrants, where it manufactured and sold a phone used by an ISIL-inspired terrorist, where it owns and licensed the software used to further the criminal enterprise, where it retains exclusive control over the source code necessary to modify and install the software, and where that very software now must be used to enable the search ordered by the warrant, compulsion of Apple is permissible under New York Telephone Co.

Moreover, other courts have directed All Writs Act orders based on warrants to entities that are not public utilities. For example, neither the credit card company in Hall nor the landlord in Access to Videotapes was a public utility. See Hall, 583 F. Supp. at 722; Access to Videotapes, 2003 WL 22053105, at *3. Apple's close relationship to the iPhone and its software, both legally and technically – which are the produce of Apple's own design – makes

compelling assistance from Apple a permissible and indispensable means of executing the warrant.

3. The Order does not place an unreasonable burden on Apple

The Order has also not placed any unreasonable burden on Apple. Where, as here, compliance with the order would not require inordinate effort, no unreasonable burden can be found. See New York Telephone Co., 434 U.S. at 175 (holding that All Writs Act order was not burdensome because it required minimal effort by the company and provided for reimbursement for the company's efforts); Mountain Bell, 616 F.2d at 1132 (rejecting telephone company's argument that unreasonable burden would be imposed because of a drain on resources and possibility of system malfunctions because the "Order was extremely narrow in scope, restricting the operation to [electronic switching system] facilities, excluding the use of manual tracing, prohibiting any tracing technique which required active monitoring by company personnel, and requiring that operations be conducted 'with a minimum of interference to the telephone service'").

While the Order in this case requires Apple to provide or employ modified software, modifying an operating system - which is essentially writing software code in discrete and limited manner - is not an unreasonable burden for a company that writes software code as part of its regular business.[6] The simple fact of having to create code that may not now exist in the exact form required does not an undue burden make. In fact, providers of electronic communications

[6] Additionally, the Order provides that Apple may request reasonable reimbursement for expenses incurred in complying with the Order.

services and remote computing services are sometimes required to write some amount of code in order to gather information in response to subpoenas or other process. Additionally, assistance under the All Writs Act has been compelled to provide something that did not previously exist - the decryption of the contents of devices seized pursuant to a search warrant. In United States v. Fricosu, 841 F.Supp.2d 1232, 1237 (D. Co. 2012), a defendant's computer – whose contents were encrypted – was seized, and the defendant was ordered pursuant to the All Writs Act to assist the government in producing a copy of the unencrypted contents of the computer. Here, the type of assistance does not even require Apple to assist in producing the unencrypted contents; the assistance is rather to facilitate the FBI's attempts to test passcodes.

As noted above, Apple designs and implements all of the features discussed, writes and cryptographically signs the iOS, routinely patches security or functionality issues in its operating system, and releases new versions of its operating system to address issues. By comparison, writing a program that turns off non-encryption features that Apple was responsible for writing to begin with would not be unduly burdensome. At no point has Apple ever said that it does not have the technical ability to comply with the Order, or that the Order asks Apple to undertake an unreasonably challenging software development task. On this point, Apple's silence speaks volumes.

Moreover, contrary to Apple's recent public statement that the assistance ordered by the Court "could be used over and over again, on any number of devices" and that "[t]he government is asking Apple to hack our own users," the Order is tailored for and limited to this particular phone. And the Order will facilitate only the FBI's

efforts to search the phone; it does not require Apple to conduct the search or access any content on the phone. Nor is compliance with the Order a threat to other users of Apple products. Apple may maintain custody of the software, destroy it after its purpose under the Order has been served, refuse to disseminate it outside of Apple, and make clear to the world that it does not apply to other devices or users without lawful court orders. As such, compliance with the Order presents no danger for any other phone and is not "the equivalent of a master key, capable of opening hundreds of millions of locks."

To the extent that Apple claims that the Order is unreasonably burdensome because it undermines Apple's marketing strategies or because it fears criticism for providing lawful access to the government, these concerns do not establish an undue burden. The principle that "private citizens have a duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions." New York Telephone 434 U.S. at 176 n.24. Apple is not above the law in that regard, and it is perfectly capable of advising consumers that compliance with a discrete and limited court order founded on probable cause is an obligation of a responsible member of the community. It does not mean the end of privacy. As discussed above, the Order requires Apple to assist only in facilitating proper, legal access based on a finding of probable cause. Further, the government is not seeking to "break" Apple's encryption infrastructure or unlawfully violate the privacy of its customers. Instead, through proper legal process through the Court, the government is seeking to use capabilities that Apple has purposefully retained in a situation where the former user of the

phone is dead and no longer has any expectation of privacy in the phone, and the owner of the phone consents both to the search of the phone and to Apple's assistance thereto.

More generally, the burden associated with compliance with legal process is measured based on the direct costs of compliance, not on other more general considerations about reputations or the ramifications of compliance. See In re XXX, 2014 WL 5510865, at *2. For example, an All Writs Act order may be used to require the production of a handwriting exemplar, see United States v. Li, 55 F.3d 325, 329 (7th Cir. 1995), even though the subject may face criminal sanctions as a result of his compliance. Apple's speculative policy concerns regarding possible consequences from compliance with the Order in this matter merit little weight, particularly when complying with a court order based on a warrant serves the ends of justice and protects public safety in furthering the investigative aims of a terrorism investigation.

4. Apple's assistance is necessary to effectuate the warrant

Apple's assistance is also necessary to effectuate the warrant. In New York Telephone Co., the Court held that the order met that standard because "[t]he provision of a leased line by the Company was essential to the fulfillment of the purpose — to learn the identities of those connected with the gambling operation — for which the pen register order had been issued." 434 U.S. at 175. The Order issued here also meets this standard, as it is essential to ensuring that the government is able to execute the warrant.

In this case, the ability to perform the search ordered by the warrant on the SUBJECT DEVICE is of critical importance to an ongoing

terrorism investigation. The user of the phone, Farook, is a mass murderer who caused the death of a large number of his coworkers and the shooting of many others, and who built bombs and hoarded weapons for this purpose. The FBI has been able to obtain several iCloud backups for the SUBJECT DEVICE, and executed a warrant to obtain all saved iCloud data associated with the SUBJECT DEVICE. Evidence in the iCloud account indicates that Farook was in communication with victims who were later killed during the shootings perpetrated by Farook on December 2, 2015, and toll records show that Farook communicated with Malik using the SUBJECT DEVICE. Importantly, however, the most recent backup of the iCloud data obtained by the government was dated October 19, 2015, approximately one and a half months before the shooting. As such, there may be relevant, critical communications and data around the time of the shooting that may reside solely on the SUBJECT DEVICE and can only be obtained if the government is able to search the phone as directed by the warrant.

Moreover, as discussed above, Apple's assistance is necessary because without the access to Apple's software code and ability to cryptographically sign code for the SUBJECT DEVICE that only Apple has, the FBI cannot attempt to determine the passcode without fear of permanent loss of access to the data or excessive time delay. Indeed, after reviewing a number of other suggestions to obtain the data from the SUBJECT DEVICE with Apple, technicians from both Apple and the FBI agreed that they were unable to identify any other methods - besides that which is now ordered by this Court - that are feasible for gaining access to the currently inaccessible data on the

SUBJECT DEVICE.[7] There can thus be no question that Apple's assistance is necessary, and that the Order was therefore properly issued.

5. Apple's Potential Marketing Concerns Provide Insufficient Grounds to Disregard a Duly Issued Court Order Following a Warrant Based on a Finding of Probable Cause

To the extent that Apple objects on the grounds that it would undermine its marketing strategy to comply with this Court's Order, or that it has an overall objection to anything that enables lawful access by the government to encrypted information, the government believes these objections are irrelevant and not legally cognizable before this Court.

First, in this case, the government seeks to search the SUBJECT DEVICE pursuant to a validly-issued search warrant, and a validly-issued All Writs Act Order. The government shares Apple's stated concern that "information needs to be protected from hackers and

---

[7] The four suggestions that Apple and the FBI discussed (and their deficiencies) were: (1) to obtain cell phone toll records for the SUBJECT DEVICE (which, while the government has of course done so, is insufficient because there is far more information on the SUBJECT DEVICE than simply toll records); (2) to determine if any computers were paired with the SUBJECT DEVICE to obtain data (which the government has determined that none were); (3) to attempt an auto-backup of the SUBJECT DEVICE with the related iCloud account (which would not work in this case because neither the owner nor the government knew the password to the iCloud account, and the owner, in an attempt to gain access to some information in the hours after the attack, was able to reset the password remotely, but that had the effect of eliminating the possibility of an auto-backup); and (4) obtaining previous back-ups of the SUBJECT DEVICE (which the government has done, but is insufficient because these backups end on October 19, 2015, nearly one-and-a-half months prior to the IRC shooting incident, and also back-ups do not appear to have the same amount of information as is on the phone itself). After subsequent conversations, though, Apple conceded that none of these suggestions would work to execute the search warrant or to sufficiently obtain the information sought.

criminals who want to access it, steal it, and use it without our knowledge or permission." See Exhibit 1. The Order at issue does not compromise that interest. This is not a situation of protecting the owner and user of this particular device against unauthorized or unlawful access - here, the owner consented to the government accessing it. Nor is it about protecting Apple's customers from the government "intercept[ing] [their] messages, access[ing] [their] health records or financial data, track[ing] [their] location, or even access [their] phone's microphone or camera without [their] knowledge" or from "hackers and criminals who want to access [personal information], steal it, and use it without our knowledge or permission." What is at stake are two judicially issued orders: one based on a finding of probable cause, approved by this Court, permitting the government to search one telephone of an individual suspected of being involved in a terrorist attack that killed 14 Americans and wounded 22 others on our own soil, the other directing Apple to provide limited assistance it is uniquely qualified to provide to effectuate that order.

Second, the assistance ordered is not a "back door" or a "hack" to all of Apple's encryption software. That is an unwarranted and inaccurate characterization. As was made plain in the government's application for the All Writs Act Order, the government asks that Apple assist in the execution of a search warrant using the capabilities that Apple has retained along within its encryption software, such that the government can attempt to determine the passcode without the additional, non-encryption features that Apple has coded into its operating system, for the SUBJECT DEVICE only. In sum, the government seeks the ability to make multiple attempts at

determining the passcode without risk that the data subject to search under the warrant would be rendered permanently inaccessible after 10 wrong attempts. This aspect of the Order is no more or less than what a user has the ability to do if the auto-erase function is turned off. Moreover, the software required is no more of a "hack" or a provision of dangerous malware than any update Apple or other providers send to a phone. Indeed, it is less so because the software requested would not reside permanently on the SUBJECT DEVICE, and Apple can retain control over it entirely. The Order does nothing regarding the encryption aspect of the operating software, but instead implicates only the non-encryption additional features that Apple has programmed.

Moreover, to the extent that Apple has concerns about turning over software to the government so that the government can run the passcode check program, the Order permits Apple to take possession of the SUBJECT DEVICE to load the programs in its own secure location, similar to what Apple has done for years for earlier operating systems, and permit the government to make its passcode attempts via remote access. In this fashion, just as with Apple's own already-existing operating systems and software, no one outside Apple would have access to the software required by the Order unless Apple itself chose to share it. This eliminates any danger that the software required by the Order would go into the "wrong hands" and lead to criminals' and bad actors' "potential to unlock any iPhone in someone's physical possession."

Third, marketing or general policy concerns are not legally cognizable objections to the Order. As discussed above, the analysis of whether a court order presents an unreasonable burden is focused

on the direct costs of compliance, not whether the party strongly disagrees with the concept of complying. This Court should not entertain an argument that fulfilling basic civic responsibilities of any American citizen or company - complying with a lawful court order - could be obviated because that company prefers to market itself as providing privacy protections that make it infeasible to comply with court-issued warrants.

6. Public Policy Favors Enforcing of the Order

Strong public policy interests favor enforcing the All Writs Act Order in this matter. In New York Telephone Co., the Supreme Court emphasized "the clear indication by Congress that the pen register is a permissible law enforcement tool." 434 U.S. at 176. Here, this matter involves the most fundamental investigative tool of all, the search warrant. Its use is enshrined in the text of the Constitution and explicitly endorsed by Congress. See U.S. Const. amend. IV ("no Warrants shall issue, but upon probable cause"); 18 U.S.C. § 3103a(a) ("a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense"). Recently, in Riley v. California, 134 S. Ct. 2473, 2495 (2014), the Supreme Court set the standard for what law enforcement must do to search a cell phone seized incident to arrest: "get a warrant." Here, the government has obtained a warrant to search the phone of a mass murderer, but unless this Court enforces the Order requiring Apple's assistance, the warrant will be meaningless.

B. Congress has Not Limited this Court's Authority to Issue an All Writs Act Order to Apple

Based on the government's discussions with Apple, Apple's public statement, and the litigation pending in the Eastern District of New

York, it appears Apple is arguing that it is justified in refusing to comply with the Order because the All Writs Act has been limited by Congress. This argument fails because there is no statute that specifically addresses the issue of Apple's assistance, and the absence of such a specific statute cannot be read as a decision to limit existing authority. Thus, the Order was an appropriate execution of this court's jurisdiction in this matter.

1. No statute addresses data extraction from a passcode-locked cell phone

The Supreme Court has made clear that "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute[,]" such that courts may not rely on the All Writs Act "[w]here a statute specifically addresses the particular issue at hand[.]" Pennsylvania Bureau of Correction, 474 U.S. at 43. In this case, no other statute addresses the procedures for requiring Apple to extract data from a passcode-locked iPhone, so Pennsylvania Bureau of Correction provides no basis for denying the government's application for an All Writs Act Order in this case.

In particular, neither Federal Rule of Criminal Procedure 41 nor the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1002, "specifically addresses" – or even vaguely addresses – the duty of Apple to assist in extracting data from a passcode-locked cell phone in order to permit the government to execute a validly issued search warrant. CALEA requires telecommunications carriers to retain the capability to comply with court orders for real-time interceptions and call-identifying information (data "in motion").[8]

[8] For example, for the contents of communications, CALEA requires telecommunications carriers to be able "to intercept" wire

(footnote cont'd on next page)

Id. By contrast, this case involves evidence already stored on a cell phone (data "at rest"). Here, Apple is not acting as a telecommunications carrier, and the Order concerns access to stored data rather than real-time interceptions and call-identifying information. Put simply, CALEA is entirely inapplicable to the present dispute and does not limit this Court's authority under the All Writs Act to require Apple to assist the government in executing a search warrant.[9]

New York Telephone Co. further illustrates that it is appropriate for a court to rely on the All Writs Act unless a statute specifically addresses the particular issue at hand. When the Court decided New York Telephone Co. in 1977, Congress had enacted Title III for intercepting the contents of communications, but it had not yet enacted the closely-related pen register statute for acquiring non-content information. See Electronic Communications Privacy Act of 1986 § 301, 100 Stat. 1848 (enacting pen register statute). Despite the existence of a statute regulating government access to information closely related to pen registers, but not specifically

---

and electronic communications carried by the carrier. 47 U.S.C. § 1002(a)(1). CALEA incorporates the definition of "intercept" from the Wiretap Act, see 47 U.S.C. § 1001(1) & 18 U.S.C. § 2510(4), and that definition encompasses only information acquired during transmission, not while it is in storage. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877-878 (9th Cir. 2002).

[9] Furthermore, nothing in CALEA prevents a court from ordering a telecommunications carrier to decrypt communications that the carrier is capable of decrypting. See 47 U.S.C. § 1002(b)(3). When Congress enacted CALEA, it understood that existing provider-assistance provisions required a provider to decrypt communications when it was able to do so. Both the House and Senate reports for CALEA stated that "telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it." H.R. Rep. No. 103-827(I), at 24 (1994); S. Rep. No. 103-402, at 24 (1994).

addressing pen registers, the Supreme Court held that an All Writs Act order could be issued in support of a warrant for a pen register. Under this reasoning, CALEA is no barrier to the Order in this case.

2. Congressional inaction does not deprive courts of their authority under the All Writs Act

The current lack of congressional action regarding encryption-related issues does not deprive this Court of its authority to issue the Order in this case. Under Pennsylvania Bureau of Correction, courts may not rely on the All Writs Act where "a statute specifically addresses" an issue. But the opposite is not true. Courts may not categorically refuse to rely on the All Writs Act - as Apple would seemingly want the Court to do - where Congress has declined to legislate. Court authority to issue All Writs Act orders in support of warrants has been clearly established since the Supreme Court decided New York Telephone Co. in 1977. Congress may choose to expand or limit this authority, but it must do so through enactment of legislation.

The Supreme Court and the Ninth Circuit have repeatedly cautioned that "Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction[.]" General Construction Company v. Castro, 401 F.3d 963, 970-71 (9th Cir. 2005) (quoting Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164, 187 (1994)); see also United States v. Craft, 535 U.S. 274, 287 (2002).

Here, there are many possible explanations for congressional inaction on encryption, including that Congress is satisfied with existing authorities, or that Congress has not yet reached agreement on whether or how much to expand existing authorities. These

possibilities provide no basis for restricting legal authorities that existed before the beginning of the debate.[10] Because courts do not lose an authority to issue orders under the All Writs Act merely because Congress does not subsequently enact legislation endorsing or expanding that authority, this Court retains authority to issue an All Writs Act Order consistent with New York Telephone Co.

IV. CONCLUSION

This Court issued a valid Order pursuant to the All Writs Act requiring Apple to assist the United States in enabling the search for evidence pursuant to a lawful search warrant. Apple has publicly stated that it will oppose this Order, and has not agreed to comply. For the foregoing reasons, the government respectfully requests that this Court issue an Order compelling Apple to comply.

[10] Granting legal force to statements or proposals by individual members of Congress during the course of congressional debate risks absurd results. Congress routinely debates and fails to act on important issues, but the mere debate does not restrict existing legal authority. Under the Constitution, Congress speaks with legal force only when it speaks as one body, through bicameralism and presentment — i.e. when it passes a bill.

EXHIBIT 1

February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.

The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.

We are challenging the FBI's demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.

Tim Cook

CERTIFICATE OF SERVICE

I, **REBECCA EVANS,** declare:

That I am a citizen of the United States and resident or employed in Riverside County, California; that my business address is the Office of United States Attorney, 3403 Tenth Street, Suite 200, Riverside, CA 92501; that I am over the age of eighteen years, and am not a party to the above-entitled action; That I am employed by the United States Attorney for the Central District of California who is a member of the Bar of the United States District Court for the Central District of California, at whose direction I served a copy:

GOVERNMENT'S MOTION TO COMPEL APPLE INC. TO COMPLY WITH THIS COURT'S FEBRUARY 16, 2016 ORDER COMPELLING ASSISTANCE IN SEARCH; EXHIBIT

[X] By electronic mail as follows:

Mr. Theodore B. Olson Gibson, Dunn & Crutcher LLP tolson@gibsondunn.com	Mr. Theodore J. Boutrous Jr. Gibson, Dunn & Crutcher LLP tboutrous@gibsondunn.com
Ms. Nicola T. Hanna Gibson, Dunn & Crutcher LLP nhanna@gibsondunn.com	Mr. Eric D. Vandevelde Gibson, Dunn & Crutcher LLP evandevelde@gibsondunn.com

This Certificate is executed on **February 19, 2016**, in Riverside, California. I certify under penalty of perjury that the foregoing is true and correct.

Rebecca Evans

REBECCA EVANS