	Case 5:16-cm-00010-SP Document 1 File	d 02/19/16 Page 1 of 35 Page ID #:1		
1	EILEEN M. DECKER United States Attorney			
2	PATRICIA A. DONAHUE Assistant United States Attorney			
3	Chief, National Security Division			
4	TRACY L. WILKISON (California Bar) Assistant United States Attorney			
5	Chief, Cyber and Intellectual Prope ALLEN W. CHIU (California Bar No. 2	erty Crimes Section		
6	Assistant United States Attorney Terrorism and Export Crimes Section			
7	1500 United States Courthouse 312 North Spring Street	Refer A		
8	Los Angeles, California 90012 Telephone: (213) 894-0622/243	35 CLEVER 06		
9	Facsimile: (213) 894-8601 Email: Tracy.Wilkison@uso	· · · · · · · · · · · · · · · · · · ·		
10	Allen.Chiu@usdoj.g			
11	Attorneys for Applicant UNITED STATES OF AMERICA			
12	UNITED STATES DISTRICT COURT			
13	FOR THE CENTRAL DISTRICT OF CALIFORNIA			
14	IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING	CM 16-10 ED No. (SP)		
15	THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300,	GOVERNMENT'S MOTION TO COMPEL		
16	CALIFORNIA LICENSE PLATE	APPLE INC. TO COMPLY WITH THIS COURT'S FEBRUARY 16, 2016 ORDER		
17	35KGD203	COMPELLING ASSISTANCE IN SEARCH; EXHIBIT		
18		Hearing Date: March 22, 2016		
19		Hearing Time: 1:00 p.m. Location: Courtroom of the Hon.		
20		Sheri Pym		
21				
22	The United States of America,	by and through its counsel of		
23	record, the United States Attorney for the Central District of			
24	California, and Assistant United States Attorneys Tracy L. Wilkison			
25	and Allen W. Chiu, hereby files its	Motion to Compel Apple Inc.		
26	("Apple") to Comply with this Court's February 16, 2016 Order			
27	Compelling Apple To Assist Agents In Its Search.			
28				

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 2 of 35 Page ID #:2

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,		
7	Dacea. repruary 19,	2016	Respectfully submitted,
8			EILEEN M. DECKER United States Attorney
9			PATRICIA A. DONAHUE
10			Assistant United States Attorney Chief, National Security Division
11			1
12			Tracy Wilke
13			TRACY L/ WILKISON ALLEN W. CHIU
14			Assistant United Attates Attorneys
15			Attorneys for Applicant UNITED STATES OF AMERICA
16			SATILD DIMINS OF AMERICA
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			2

	Case	5:16-c	:m-000	10-SP Document 1 Filed 02/19/16 Page 3 of 35 Page ID #:3
1				TABLE OF CONTENTS
2	DESC	RIPTI	ON	PAGE
3	TABL	E OF .	AUTHOI	RITIESii
4	MEMO	RANDUI	MOFI	POINTS AND AUTHORITIES1
5	I.	INTR	ODUCT	ION1
6	II.	STAT	EMENT	OF FACTS
7 8	III.	WITH	ITS (SHOULD ISSUE AN ORDER COMPELLING APPLE TO COMPLY ORDER REQUIRING ASSISTANCE WITH THE FBI'S SEARCH BJECT DEVICE PURSUANT TO THE ALL WRITS ACT
9		А.	This	Court's All Writs Act Order is Lawful and Binding7
10			1.	The All Writs Act7
11			2.	Apple is not "far removed" from this matter10
12			3.	The Order does not place an unreasonable burden
13				on Apple12
14			4.	Apple's assistance is necessary to effectuate the warrant16
15 16			5.	Apple's Potential Marketing Concerns Provide Insufficient Grounds to Disregard a Duly Issued Court Order Following a Warrant Based on a
17				Finding of Probable Cause18
18			6.	Public Policy Favors Enforcing of the Order21
19		В.	Congr Issue	ress has Not Limited this Court's Authority to an All Writs Act Order to Apple
20 21			1.	No statute addresses data extraction from a passcode-locked cell phone22
22			2.	Congressional inaction does not deprive courts of their authority under the All Writs Act24
23	IV.	CONCI	LUSION	J
24				
25				
26				
27				
28				
				i

	Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 4 of 35 Page ID #:4
1	TABLE OF AUTHORITIES
2	DESCRIPTION
3	FEDERAL CASES
4	Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164 (1994)24
5	General Construction Company v. Castro,
6	401 F.3d 963 (9th Cir. 2005)24
7 8	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
9	(D.P.R. Aug. 27, 2015)
10	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 (9th Cir. 1980)passim
11	In re Application of United States for an Order Directing X to
12	Provide Access to Videotapes (Access to Videotapes), 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003)
13	(unpublished)
14 15	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.
16	Oct. 31, 2014)9, 15
17	Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)22
18	Pennsylvania Bureau of Correction v. United States Marshals Service,
19	474 U.S. 34 (1985)
20	Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283 (9th Cir. 1979)7
21	Riley v. California,
22	134 S. Ct. 2473 (2014)
23	United States v. Catoggio, 698 F.3d 64 (2d Cir. 2012)8
24	United States v. Craft,
25 26	535 U.S. 274 (2002)
26	United States v. Fricosu, 841 F.Supp.2d 1232 (D. Co. 2012)17
28	ii

	Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 5 of 35 Page ID #:5
1	United States v. Hall, 583 F. Supp. 717 (E.D. Va. 1984)
2	United States v. Li.
3	55 F.3d 325, 329 (7th Cir. 1995)15
4	United States v. Navarro, No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013)
5	United States v. New York Telephone Co., 434 U.S. 159 (1977)passim
6	
7	FEDERAL STATUTES
8	18 U.S.C. § 2510
9	18 U.S.C. § 3103
10	28 U.S.C. § 1651
11	47 U.S.C. § 1001
12	47 U.S.C. § 1002
13	
14	
15	
16	
17 18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	iii

1

MEMORANDUM OF POINTS AND AUTHORITIES

2 I. INTRODUCTION

Rather than assist the effort to fully investigate a deadly 3 terrorist attack by obeying this Court's Order of February 16, 2016, 4 Apple has responded by publicly repudiating that Order. See Exhibit 5 1. Apple has attempted to design and market its products to allow 6 technology, rather than the law, to control access to data which has 7 been found by this Court to be warranted for an important 8 9 investigation. Despite its efforts, Apple nonetheless retains the technical ability to comply with the Order, and so should be required 10 to obey it. 11

Before Syed Rizwan Farook ("Farook") and his wife Tafsheen Malik 12 13 shot and killed 14 people and injured 22 others at the Inland Regional Center in San Bernardino, Farook's employer issued him an 14 15 iPhone. The Federal Bureau of Investigation ("FBI") recovered that iPhone during the investigation into the massacre. The government 16 17 has reason to believe that Farook used that iPhone to communicate 18 with some of the very people whom he and Malik murdered. The phone may contain critical communications and data prior to and around the 19 time of the shooting that, thus far: (1) has not been accessed; (2) 20 may reside solely on the phone; and (3) cannot be accessed by any 21 22 other means known to either the government or Apple. The FBI obtained a warrant to search the iPhone, and the owner of the iPhone, 23 24 Farook's employer, also gave the FBI its consent to the search. Because the iPhone was locked, the government subsequently sought 25 Apple's help in its efforts to execute the lawfully issued search 26 warrant. Apple refused. 27

Apple left the government with no option other than to apply to 1 2 this Court for the Order issued on February 16, 2016. The Order requires Apple to assist the FBI with respect to this single iPhone 3 used by Farook by providing the FBI with the opportunity to determine 4 5 the passcode. The Order does not, as Apple's public statement alleges, require Apple to create or provide a "back door" to every 6 iPhone; it does not provide "hackers and criminals" access to 7 iPhones; it does not require Apple to "hack [its] own users" or to 8 9 "decrypt" its own phones; it does not give the government "the power 10 to reach into anyone's device" without a warrant or court authorization; and it does not compromise the security of personal 11 12 information. See Exhibit 1. To the contrary, the Order allows Apple to retain custody of its software at all times, and it gives Apple 13 14 flexibility in the manner in which it provides assistance. In fact, the software never has to come into the government's custody. 15

In the past, Apple has consistently complied with a significant 16 number of orders issued pursuant to the All Writs Act to facilitate 17 the execution of search warrants on Apple devices running earlier 18 versions of iOS.¹ The use of the All Writs Act to facilitate a 19 20 warrant is therefore not unprecedented; Apple itself has recognized 21 it for years. Based on Apple's recent public statement and other statements by Apple, Apple's current refusal to comply with the 22 23 Court's Order, despite the technical feasibility of doing so, instead

²⁴

¹ Apple's Legal Process Guidelines continue to state that Apple will provide assistance with unlocking devices running iOS versions 25 earlier than 8.0, and advises as to what language to include in the order. See "Extracting Data from Passcode Locked iOS Devices," Apple 26 Legal Process Guidelines § III(I) (updated September 29, 2015), available at http://www.apple.com/privacy/docs/legal-process-27 guidelines-us.pdf. However, Apple has informed another court that it

now objects to providing such assistance. 28

appears to be based on its concern for its business model and public 1 2 brand marketing strategy.²

3 Accordingly, the government now brings this motion to compel. 4 While the Order includes the provision that "to the extent that Apple believes that compliance with this Order would be unreasonably 5 burdensome, it may make an application to this Court for relief 6 within five business days of receipt of the Order," Apple's public 7 8 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 9 heard, and expects these issues to be fully briefed before the Court; 10 however, the urgency of this investigation requires this motion now 11 12 that Apple has made its intention not to comply patently clear.³ This aspect of the investigation into the December 2, 2015 terrorist 13 attack must move forward. 14

15 II. STATEMENT OF FACTS

16 As set forth in the government's application for the All Writs 17 Act Order, and the Declaration of FBI Supervisory Special Agent ("SSA") Christopher Pluhar, which was attached thereto, both of which 18 were filed on February 16, 2016, the FBI has been investigating the 19

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 "[0]pposing [of] this order" and its 26 stated interest in adversarial testing of the order's legal merits, 27 the government files this noticed motion to provide Apple with the due process and adversarial testing it seeks. 28

²⁰

² As Apple has stated on its web page, "Our commitment to customer privacy doesn't stop because of a government information 21 request. ... Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically 22 feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS8." 23 (https://web.archive.org/web/20140918023950/http://www.apple.com/priv acy/government-informaton-requests/). Notably, notwithstanding this 24 previous statement, Apple concedes that it has retained the ability to do as the Court ordered. 25

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 б precise role of those who may have been involved in the attack. As 7 part of this investigation, the FBI obtained search warrants to 8 search, among other locations and items, the digital devices and 9 online accounts of Farook and Malik. Through those searches, the FBI 10 has discovered crucial information about the attack. For example, 11 the FBI discovered that on December 2, 2015, at approximately 11:14 12 13 a.m., a post on a Facebook page associated with Malik stated, "We pledge allegiance to Khalifa bu bkr al bhaghdadi al quraishi," 14 referring to Abu Bakr Al Baghdadi, the leader of Islamic State of 15 16 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. 17 ISIL is designated as a foreign terrorist organization by the United 18 19 States Department of State and has been so designated since December 20 2004. Moreover, a search warrant executed at Farook's residence resulted in the discovery of thousands of rounds of ammunition and 21 22 over a dozen pipe bombs.

In addition, as part of the FBI's investigation, on December 3, 24 2015, the Honorable David T. Bristow, United States Magistrate Judge, 25 issued a search warrant in Docket Number ED 15-0451M for a black 26 Lexus IS300, which was a vehicle that Farook used. The vehicle was 27 parked outside of his residence where the thousands of rounds of 28 ammunition and pipe bombs were found. The search warrant for the

vehicle also ordered the search of digital devices located within it. 1 Inside the vehicle the FBI found a cellular telephone of an Apple 2 make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, 3 IMEI:358820052301412, on the Verizon Network (the "SUBJECT DEVICE"). 4 The SUBJECT DEVICE is owned by Farook's employer at the San 5 Bernardino County Department of Public Health ("SBCDPH"), and was б assigned to, and used by, Farook as part of his employment. 7 The 8 SBCDPH provided the government its consent to search the SUBJECT 9 DEVICE and to Apple's assistance with that search.⁴

Nonetheless, despite the search warrant ordered by the Court and 10 the owner's consent to search the SUBJECT DEVICE, the FBI has been 11 unable to search the SUBJECT DEVICE because it is "locked" or secured 12 with a user-determined, numeric passcode. More to the point, the FBI 13 has been unable to make attempts to determine the passcode to access 14 the SUBJECT DEVICE because Apple has written, or "coded," its 15 operating systems with a user-enabled "auto-erase function" that 16 would, if enabled, result in the permanent destruction of the 17 required encryption key material after 10 failed attempts at the 18 entering the correct passcode (meaning that, after 10 failed 19 20 attempts, the information on the device becomes permanently inaccessible). 21

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

^{27 &}lt;sup>4</sup> In addition, SBCDPH has a written policy that all digital devices are subject to search at any time by the SBCDPH, which 28 Farook accepted via signature upon employment.

shootings on December 2, 2015, the backup iCloud data which the 1 2 government has been able to obtain for the account ends on October 19, 2015. In addition, toll records for the SUBJECT DEVICE establish 3 that Farook communicated with Malik using the SUBJECT DEVICE between 4 July and November 2015, but this information is not found in the 5 backup iCloud data. Accordingly, there may be critical 6 communications and data prior to and around the time of the shooting 7 8 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 9 government or Apple. 10

When the government first realized that Apple retained the means 11 to obtain that data from the SUBJECT DEVICE and that due to the way 12 that Apple created the software Apple was the only means of obtaining 13 that data, the government sought Apple's voluntary assistance. Apple 14 rejected the government's request, although it conceded that it had 15 the technical capability to help. As a result, without any other 16 alternative, on February 16, 2016, the government applied for - and 17 this Court subsequently issued - an Order pursuant to the All Writs 18 Act, compelling Apple to assist the FBI in its search of the SUBJECT 19 20 DEVICE.

After the government served this Court's Order on Apple, Apple 21 issued a public statement responding directly to the Order. 22 See 23 Exhibit 1. In that statement, Apple again did not assert that it lacks the technical capability to execute the Order, that it is not 24 25 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 26 combination of: a perceived negative impact on its reputation and 27 marketing strategy were it to provide the ordered assistance to the 28

б

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page-12 of 35 Page ID #:12

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

3

4

5

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

To the extent that Apple objects that the Court does not have 6 authority under the All Writs Act to compel Apple to assist in the 7 execution of a lawfully obtained search warrant, this objection fails 8 because the authority to require reasonable third-party assistance 9 that is necessary to execute a warrant is well-established, and no 10 provision of any other law or any judicial decision justifies 11 limitation of that All Writs Act authority. To allow Apple not to 12 comply with the Order would frustrate the execution of a valid 13 warrant and thwart the public interest in a full and complete 14 investigation of a horrific act of terrorism. 15

16

1. The All Writs Act

17 The All Writs Act provides in relevant part that "all courts established by Act of Congress may issue all writs necessary or 18 19 appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the 20 Supreme Court explained, "[t]he All Writs Act is a residual source of 21 authority to issue writs that are not otherwise covered by statute." 22 Pennsylvania Bureau of Correction v. United States Marshals Service, 23 474 U.S. 34, 43 (1985). Pursuant to the All Writs Act, the Court has 24 25 the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement 26 Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th officers." 27 Cir. 1979) (citing United States v. New York Telephone Co., 434 U.S. 28

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 13 of 35 Page ID #:13

1 159 (1977)). The All Writs Act permits a court, in its "sound judgment," to issue orders necessary "to achieve the rational ends of 2 law" and "the ends of justice entrusted to it." New York Telephone 3 Co., 434 U.S. at 172-73 (citations and internal quotation marks 4 omitted). Courts must apply the All Writs Act "flexibly in 5 conformity with these principles." Id. at 173; accord United States 6 7 v. Catoggio, 698 F.3d 64, 67 (2d Cir. 2012) ("[C]ourts have significant flexibility in exercising their authority under the 8 9 Act.") (citation omitted).

In New York Telephone Co., the Supreme Court held that courts 10 have authority under the All Writs Act to issue supplemental orders 11 to third parties to facilitate the execution of search warrants. 12 The Court held that "[t]he power conferred by the Act extends, under 13 appropriate circumstances, to persons who, though not parties to the 14 original action or engaged in wrongdoing, are in a position to 15 frustrate the implementation of a court order or the proper 16 administration of justice, ... and encompasses even those who have not 17 taken any affirmative action to hinder justice." Id. at 174. In 18 particular, the Court upheld an order directing a phone company to 19 assist in executing a pen register search warrant issued under Rule 20 See id. at 171-76; see also In re Application of United States 21 41. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over 22 23 Tel. Facilities (Mountain Bell), 616 F.2d 1122, 1132-33 (9th Cir. 1980) (affirming district court's order compelling Mountain Bell to 24 trace telephone calls, on grounds that "the obligations imposed . . . 25 were reasonable ones." (citing New York Telephone Co., 434 U.S. at 26 27 172)). New York Telephone Co. also held that "Rule 41 is not limited to tangible items but is sufficiently flexible to include within its 28

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 14 of 35 Page ID #:14

1 scope electronic intrusions authorized upon a finding of probable cause." 434 U.S. at 169. The Court relied upon the authority of a 2 search warrant pursuant to Rule 41 to predicate an All Writs Act 3 4 order commanding a utility to implement a pen register and trap and trace device - before Congress had passed a law that specifically 5 authorized pen registers by court order. Under New York Telephone 6 Co. and Mountain Bell, the Court had authority pursuant to the All 7 8 Writs Act to issue the Order.

9 Further, based on the authority given under the All Writs Act. courts have issued orders, similar to the one the Court issued here, 10 that require a manufacturer to attempt to assist in accessing a 11 12 cellphone's image files so that a warrant may be executed as originally contemplated. See, e.g., In re Order Requiring [XXX], 13 Inc. to Assist in the Execution of a Search Warrant Issued by This 14 15 Court by Unlocking a Cellphone (In re XXX), 2014 WL 5510865, at *2 16 (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 17 issued All Writs Act orders in support of warrants in a wide variety 18 of contexts, including ordering a phone company to assist with a trap 19 and trace device (Mountain Bell, 616 F.2d at 1129); ordering a credit 20 card company to produce customer records (United States v. Hall, 583 21 22 F. Supp. 717, 722 (E.D. Va. 1984)); ordering a landlord to provide access to security camera videotapes (In re Application of United 23 States for an Order Directing X to Provide Access to Videotapes 24 25 (Access to Videotapes), 2003 WL 22053105, at *3 (D. Md. Aug. 22, 26 2003) (unpublished)); and ordering a phone company to assist with 27 consensual monitoring of a customer's calls (In re Application of the United States for an Order Directing a Provider of Communication 28

Services to Provide Technical Assistance to the DEA, 2015 WL 5233551, 1 2 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 3 country compelling Apple to assist in the execution of a search 4 warrant by accessing the data on devices running earlier versions of 5 iOS, orders with which Apple complied.⁵ In fact, as noted above, 6 Apple has long recognized this application, and has complied with 7 8 search warrants compelling Apple to extract data from older iOS devices locked with a passcode. Until last year, Apple did not 9 dispute any such order. 10

In New York Telephone Co., the Supreme Court considered three 11 factors in concluding that the issuance of the All Writs Act order to 12 13 the phone company was appropriate. First, it found that the phone 14 company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." Id. at 174. 15 Second, it concluded that the order did not place an undue burden on 16 the phone company. See id. at 175. Third, it determined that the 17 assistance of the company was necessary to achieve the purpose of the 18 warrant. See id. As set forth below, each of these factors supports 19 the order issued in this case. 20

21

24

2. <u>Apple is not "far removed" from this matter</u>

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 <u>sua sponte</u> 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 1 and owns the software that runs the phone - which software is 2 preventing the search for evidence authorized by the warrant. 3 Indeed, Apple has positioned itself to be essential to gaining access 4 to the SUBJECT DEVICE or any other Apple device, and has marketed its 5 products on this basis. See, e.g., Apple's Security Guide, 6 www.apple.com/business/docs/iOS Security Guide.pdf. Apple designed 7 and restricts access to the code for the auto-erase function - the 8 function that makes the data on the phone permanently inaccessible 9 after multiple failed passcode attempts. This feature effectively 10 prevents the government from performing the search for evidence 11 authorized by the warrant without Apple's assistance. The same 12 software Apple is uniquely able to modify also controls the delays 13 Apple implemented between failed passcode attempts - which makes the 14 process take too long to enable the access ordered by the Court. 15 Especially but not only because iPhones will only run software 16 17 cryptographically signed by Apple, and because Apple restricts access to the source code of the software that creates these obstacles, no 18 19 other party has the ability to assist the government in preventing 20 these features from obstructing the search ordered by the Court pursuant to the warrant. Just because Apple has sold the phone to a 21 customer and that customer has created a passcode does not mean that 22 the close software connection ceases to exist; Apple has designed the 23 phone and software updates so that Apple's continued involvement and 24 connection is required. 25

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

orders to public utilities is inconsistent with the broad scope of 1 judicial authority under the All Writs Act. New York Telephone Co. 2 3 emphasized that "the Company's facilities were being employed to 4 facilitate a criminal enterprise on a continuing basis[,]" and the company's noncompliance "threatened obstruction of an investigation 5 which would determine whether the Company's facilities were being 6 lawfully used." 434 U.S. at 174. In Mountain Bell, the Ninth 7 Circuit emphasized that its decision "should not be read to authorize 8 the wholesale imposition upon private, third parties of duties 9 10 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 11 the target of the investigation. Where Apple designed its software 12 and that design interferes with the execution of search warrants, 13 where it manufactured and sold a phone used by an ISIL-inspired 14 terrorist, where it owns and licensed the software used to further 15 the criminal enterprise, where it retains exclusive control over the 16 source code necessary to modify and install the software, and where 17 that very software now must be used to enable the search ordered by 18 the warrant, compulsion of Apple is permissible under New York 19 20 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 <u>Hall</u> nor the landlord in <u>Access to</u> <u>Videotapes</u> was a public utility. <u>See Hall</u>, 583 F. Supp. at 722; <u>Access to Videotapes</u>, 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

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 18 of 35 Page ID #:18

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

3

4

3. The Order does not place an unreasonable burden on $\frac{Apple}{P}$

The Order has also not placed any unreasonable burden on Apple. 5 Where, as here, compliance with the order would not require 6 inordinate effort, no unreasonable burden can be found. See New York 7 Telephone Co., 434 U.S. at 175 (holding that All Writs Act order was 8 9 not burdensome because it required minimal effort by the company and provided for reimbursement for the company's efforts); Mountain Bell, 10 11 616 F.2d at 1132 (rejecting telephone company's argument that unreasonable burden would be imposed because of a drain on resources 12 and possibility of system malfunctions because the "Order was 13 extremely narrow in scope, restricting the operation to [electronic 14 switching system] facilities, excluding the use of manual tracing, 15 prohibiting any tracing technique which required active monitoring by 16 company personnel, and requiring that operations be conducted 'with a 17 minimum of interference to the telephone service'"). 18

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 1 2 write some amount of code in order to gather information in response 3 to subpoenas or other process. Additionally, assistance under the All Writs Act has been compelled to provide something that did not 4 previously exist - the decryption of the contents of devices seized 5 pursuant to a search warrant. In United States v. Fricosu, 841 6 7 F.Supp.2d 1232, 1237 (D. Co. 2012), a defendant's computer - whose contents were encrypted - was seized, and the defendant was ordered 8 pursuant to the All Writs Act to assist the government in producing a 9 copy of the unencrypted contents of the computer. Here, the type of 10 assistance does not even require Apple to assist in producing the 11 unencrypted contents; the assistance is rather to facilitate the 12 FBI's attempts to test passcodes. 13

As noted above, Apple designs and implements all of the features 14 discussed, writes and cryptographically signs the iOS, routinely 15 patches security or functionality issues in its operating system, and 16 releases new versions of its operating system to address issues. 17 By comparison, writing a program that turns off non-encryption features 18 19 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 20 have the technical ability to comply with the Order, or that the 21 Order asks Apple to undertake an unreasonably challenging software 22 development task. On this point, Apple's silence speaks volumes. 23

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

Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 20 of 35 Page ID #:20

efforts to search the phone; it does not require Apple to conduct the 1 2 search or access any content on the phone. Nor is compliance with the Order a threat to other users of Apple products. Apple may 3 4 maintain custody of the software, destroy it after its purpose under the Order has been served, refuse to disseminate it outside of Apple, 5 and make clear to the world that it does not apply to other devices 6 or users without lawful court orders. As such, compliance with the 7 8 Order presents no danger for any other phone and is not "the equivalent of a master key, capable of opening hundreds of millions 9 10 of locks."

To the extent that Apple claims that the Order is unreasonably 11 burdensome because it undermines Apple's marketing strategies or 12 because it fears criticism for providing lawful access to the 13 government, these concerns do not establish an undue burden. The 14 principle that "private citizens have a duty to provide assistance to 15 law enforcement officials when it is required is by no means foreign 16 to our traditions." New York Telephone 434 U.S. at 176 n.24. Apple 17 is not above the law in that regard, and it is perfectly capable of 18 advising consumers that compliance with a discrete and limited court 19 20 order founded on probable cause is an obligation of a responsible member of the community. It does not mean the end of privacy. As 21 discussed above, the Order requires Apple to assist only in 22 facilitating proper, legal access based on a finding of probable 23 cause. Further, the government is not seeking to "break" Apple's 24 25 encryption infrastructure or unlawfully violate the privacy of its 26 customers. Instead, through proper legal process through the Court, the government is seeking to use capabilities that Apple has 27 purposefully retained in a situation where the former user of the 28

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.

4 More generally, the burden associated with compliance with legal process is measured based on the direct costs of compliance, not on 5 other more general considerations about reputations or the 6 ramifications of compliance. See In re XXX, 2014 WL 5510865, at *2. 7 For example, an All Writs Act order may be used to require the 8 production of a handwriting exemplar, see United States v. Li, 55 9 10 F.3d 325, 329 (7th Cir. 1995), even though the subject may face criminal sanctions as a result of his compliance. Apple's 11 speculative policy concerns regarding possible consequences from 12 compliance with the Order in this matter merit little weight, 13 particularly when complying with a court order based on a warrant 14 serves the ends of justice and protects public safety in furthering 15 16 the investigative aims of a terrorism investigation.

- 17
- 18

4. <u>Apple's assistance is necessary to effectuate the</u> warrant

Apple's assistance is also necessary to effectuate the warrant. 19 In New York Telephone Co., the Court held that the order met that 20 standard because "[t]he provision of a leased line by the Company was 21 essential to the fulfillment of the purpose - to learn the identities 22 of those connected with the gambling operation - for which the pen 23 register order had been issued." 434 U.S. at 175. The Order issued 24 25 here also meets this standard, as it is essential to ensuring that the government is able to execute the warrant. 26

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 1 murderer who caused the death of a large number of his coworkers and 2 the shooting of many others, and who built bombs and hoarded weapons 3 for this purpose. The FBI has been able to obtain several iCloud 4 backups for the SUBJECT DEVICE, and executed a warrant to obtain all 5 saved iCloud data associated with the SUBJECT DEVICE. Evidence in 6 the iCloud account indicates that Farook was in communication with 7 victims who were later killed during the shootings perpetrated by 8 Farook on December 2, 2015, and toll records show that Farook 9 communicated with Malik using the SUBJECT DEVICE. Importantly, 10 however, the most recent backup of the iCloud data obtained by the 11 government was dated October 19, 2015, approximately one and a half 12 months before the shooting. As such, there may be relevant, critical 13 communications and data around the time of the shooting that may 14 reside solely on the SUBJECT DEVICE and can only be obtained if the 15 government is able to search the phone as directed by the warrant. 16

Moreover, as discussed above, Apple's assistance is necessary 17 because without the access to Apple's software code and ability to 18 cryptographically sign code for the SUBJECT DEVICE that only Apple 19 has, the FBI cannot attempt to determine the passcode without fear of 20 permanent loss of access to the data or excessive time delay. 21 Indeed, after reviewing a number of other suggestions to obtain the 22 23 data from the SUBJECT DEVICE with Apple, technicians from both Apple 24 and the FBI agreed that they were unable to identify any other methods - besides that which is now ordered by this Court - that are 25 feasible for gaining access to the currently inaccessible data on the 26

- 27
- 28

Case 5:16-cm-00010-SP- Document 1 Filed 02/19/16 Page-23 of 35 Page ID #:23

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

4

5

6

17

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

7 To the extent that Apple objects on the grounds that it would 8 undermine its marketing strategy to comply with this Court's Order, 9 or that it has an overall objection to anything that enables lawful 10 access by the government to encrypted information, the government 11 believes these objections are irrelevant and not legally cognizable 12 before this Court.

First, in this case, the government seeks to search the SUBJECT DEVICE pursuant to a validly-issued search warrant, and a validlyissued 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 18 their deficiencies) were: (1) to obtain cell phone toll records for the SUBJECT DEVICE (which, while the government has of course done 19 so, is insufficient because there is far more information on the SUBJECT DEVICE than simply toll records); (2) to determine if any 20 computers were paired with the SUBJECT DEVICE to obtain data (which the government has determined that none were); (3) to attempt an 21 auto-backup of the SUBJECT DEVICE with the related iCloud account (which would not work in this case because neither the owner nor the 22 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 23 attack, was able to reset the password remotely, but that had the effect of eliminating the possibility of an auto-backup); and (4) 24 obtaining previous back-ups of the SUBJECT DEVICE (which the 25 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 26 amount of information as is on the phone itself). After subsequent conversations, though, Apple conceded that none of these suggestions 27 would work to execute the search warrant or to sufficiently obtain the information sought. 28

criminals who want to access it, steal it, and use it without our 1 knowledge or permission." See Exhibit 1. The Order at issue does 2 not compromise that interest. This is not a situation of protecting 3 the owner and user of this particular device against unauthorized or 4 unlawful access - here, the owner consented to the government 5 accessing it. Nor is it about protecting Apple's customers from the 6 government "intercept[ing] [their] messages, access[ing] [their] 7 health records or financial data, track[ing] [their] location, or 8 9 even access [their] phone's microphone or camera without [their] knowledge" or from "hackers and criminals who want to access 10 [personal information], steal it, and use it without our knowledge or 11 permission." What is at stake are two judicially issued orders: one 12 13 based on a finding of probable cause, approved by this Court, permitting the government to search one telephone of an individual 14 suspected of being involved in a terrorist attack that killed 14 15 Americans and wounded 22 others on our own soil, the other directing 16 Apple to provide limited assistance it is uniquely qualified to 17 18 provide to effectuate that order.

19 Second, the assistance ordered is not a "back door" or a "hack" to all of Apple's encryption software. That is an unwarranted and 20 inaccurate characterization. As was made plain in the government's 21 application for the All Writs Act Order, the government asks that 22 23 Apple assist in the execution of a search warrant using the capabilities that Apple has retained along within its encryption 24 25 software, such that the government can attempt to determine the passcode without the additional, non-encryption features that Apple 26 27 has coded into its operating system, for the SUBJECT DEVICE only. In 28 sum, the government seeks the ability to make multiple attempts at

determining the passcode without risk that the data subject to search 1 2 under the warrant would be rendered permanently inaccessible after 10 wrong attempts. This aspect of the Order is no more or less than 3 what a user has the ability to do if the auto-erase function is 4 turned off. Moreover, the software required is no more of a "hack" 5 or a provision of dangerous malware than any update Apple or other 6 providers send to a phone. Indeed, it is less so because the 7 8 software requested would not reside permanently on the SUBJECT DEVICE, and Apple can retain control over it entirely. The Order 9 does nothing regarding the encryption aspect of the operating 10 software, but instead implicates only the non-encryption additional 11 12 features that Apple has programmed.

13 Moreover, to the extent that Apple has concerns about turning over software to the government so that the government can run the 14 passcode check program, the Order permits Apple to take possession of 15 the SUBJECT DEVICE to load the programs in its own secure location, 16 17 similar to what Apple has done for years for earlier operating systems, and permit the government to make its passcode attempts via 18 19 remote access. In this fashion, just as with Apple's own alreadyexisting operating systems and software, no one outside Apple would 20 have access to the software required by the Order unless Apple itself 21 chose to share it. This eliminates any danger that the software 22 required by the Order would go into the "wrong hands" and lead to 23 criminals' and bad actors' "potential to unlock any iPhone in 24 someone's physical possession." 25

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.

8

6. Public Policy Favors Enforcing of the Order

9 Strong public policy interests favor enforcing the All Writs Act Order in this matter. In New York Telephone Co., the Supreme Court 10 emphasized "the clear indication by Congress that the pen register is 11 a permissible law enforcement tool." 434 U.S. at 176. Here, this 12 matter involves the most fundamental investigative tool of all, the 13 search warrant. Its use is enshrined in the text of the Constitution 14 and explicitly endorsed by Congress. See U.S. Const. amend. IV ("no 15 Warrants shall issue, but upon probable cause"); 18 U.S.C. § 3103a(a) 16 ("a warrant may be issued to search for and seize any property that 17 constitutes evidence of a criminal offense"). Recently, in Riley v. 18 California, 134 S. Ct. 2473, 2495 (2014), the Supreme Court set the 19 standard for what law enforcement must do to search a cell phone 20 seized incident to arrest: "get a warrant." Here, the government 21 has obtained a warrant to search the phone of a mass murderer, but 22 unless this Court enforces the Order requiring Apple's assistance, 23 the warrant will be meaningless. 24

25

26

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.

8 9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

1. <u>No statute addresses data extraction from a passcode-</u> 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[.]" <u>Pennsylvania Bureau of Correction</u>, 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 <u>Pennsylvania Bureau of Correction</u> 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

27
⁸ For example, for the contents of communications, CALEA
28 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 1 cell phone (data "at rest"). Here, Apple is not acting as a 2 telecommunications carrier, and the Order concerns access to stored 3 data rather than real-time interceptions and call-identifying 4 information. Put simply, CALEA is entirely inapplicable to the 5 6 present dispute and does not limit this Court's authority under the 7 All Writs Act to require Apple to assist the government in executing a search warrant.⁹ 8

New York Telephone Co. further illustrates that it is 9 appropriate for a court to rely on the All Writs Act unless a statute 10 specifically addresses the particular issue at hand. When the Court 11 decided New York Telephone Co. in 1977, Congress had enacted Title 12 13 III for intercepting the contents of communications, but it had not yet enacted the closely-related pen register statute for acquiring 14 non-content information. See Electronic Communications Privacy Act 15 of 1986 § 301, 100 Stat. 1848 (enacting pen register statute). 16 Despite the existence of a statute regulating government access to 17 information closely related to pen registers, but not specifically 18

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).

19

⁹ Furthermore, nothing in CALEA prevents a court from ordering a 23 telecommunications carrier to decrypt communications that the carrier is capable of decrypting. See 47 U.S.C. § 1002(b)(3). When Congress 24 enacted CALEA, it understood that existing provider-assistance provisions required a provider to decrypt communications when it was 25 able to do so. Both the House and Senate reports for CALEA stated that "telecommunications carriers have no responsibility to decrypt 26 encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt 27 it." H.R. Rep. No. 103-827(I), at 24 (1994); S. Rep. No. 103-402, at 24 (1994). 28

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. <u>Congressional inaction does not deprive courts of</u> <u>their authority under the All Writs Act</u>

The current lack of congressional action regarding encryptionrelated issues does not deprive this Court of its authority to issue the Order in this case. Under <u>Pennsylvania Bureau of Correction</u>, 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 <u>New York Telephone Co.</u> 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[.]" <u>General Construction Company v. Castro</u>, 401 F.3d 963, 970-71 (9th Cir. 2005) (quoting <u>Central Bank of Denver v. First</u> <u>Interstate Bank of Denver</u>, 511 U.S. 164, 187 (1994)); <u>see also United</u> 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

28

4

5

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 <u>New York Telephone Co.</u>

IV. CONCLUSION

7

14

15

16

17

18

19

20

21

2.2

23

24

8 This Court issued a valid Order pursuant to the All Writs Act 9 requiring Apple to assist the United States in enabling the search 10 for evidence pursuant to a lawful search warrant. Apple has publicly 11 stated that it will oppose this Order, and has not agreed to comply. 12 For the foregoing reasons, the government respectfully requests that 13 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. Case 5:16-cm-00010-SP Document 1 Filed 02/19/16 Page 31 of 35 Page ID #:31

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.

Cuetase 5.18 cm-00010-SP Document 1 Filed 02/19/16 Page-34 of 35 Page 10 # 34 of 3

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

Shop and Learn	Apple Store	For Education	Account	About Apple
Mac	Find a Store	Apple and Education	Manage Your Apple ID	Apple Info
iPad	Genius Bar	Shop for College	Apple Store Account	Job Opportunities
iPhone	Workshops and Learning		iCloud.com	Press Info
Watch	Youth Programs	For Business		Investors
TV	Apple Store App	iPhone in Business	Apple Values	Events
Music	Refurbished	Pad in Business	Environment	Hot News
iTunes	Financing	Mac in Business	Supplier Responsibility	Legal
iPod	Reuse and Recycling	Shop for Your Business	Accessibility	Contact Apple
Accessones	Order Status		Privacy	
Gift Cards	Shopping Help		Inclusion and Diversity	
			Education	

More ways to shop their a capile Store call 1-800 MY aPPLE, or find a reseller

Copyright < 2016 Apple the All rights reserved Privacy Policy Terms of Use Sales and Refunds Site Map

United States

Case 5:16-cm-00010-SP Document 1	Filed 02/19/16	Page 35 of 35	Page ID #:35
----------------------------------	----------------	---------------	--------------

CERTIFICATE OF SERVICE

I, REBECCA EVANS, declare:

3					
4	That I am a citizen of the United States and resident or employed in Riverside				
5	County, California; that my business address is the Office of United States Attorney, 3403				
6	Tenth Street, Suite 200, Riverside, CA 92501; that I am over the age of eighteen years, and				
7	am not a party to the above-entitled action; That I am employed by the United States				
8	Attorney for the Central District of California who is a member of the Bar of the United States				
9	District Court for the Central District of California, at whose direction I served a copy:				
10 11	COVERNMENT'S MOTION TO COMPEL ADDI E INO TO COMPLY WITH THE CONTRACT				
12	GOVERNMENT'S MOTION TO COMPEL APPLE INC. TO COMPLY WITH THIS COURT'S FEBRUARY 16, 2016 ORDER COMPELLING ASSISTANCE IN SEARCH; EXHIBIT				
13	[X] By electronic mail as follows:				
14					
15	Mr. Theodore B. OlsonMr. Theodore J. Boutrous Jr.Gibson, Dunn & Crutcher LLPGibson, Dunn & Crutcher LLP				
16	tolson@gibsondunn.com tboutrous@gibsondunn.com				
17	Ms. Nicola T. HannaMr. Eric D. VandeveldeGibson, Dunn & Crutcher LLPGibson, Dunn & Crutcher LLP				
18	<u>nhanna@gibsondunn.com</u> <u>evandevelde@gibsondunn.com</u>				
19					
20 21	This Certificate is executed on February 19, 2016, in Riverside, California. I				
22	certify under penalty of perjury that the foregoing is true and correct.				
23					
24	REBECCA EVANS				
25					
26					
27					
28					

UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ED CM 16-10-SP	Date	February 18, 2016
Title	In the matter of the search of an Apple iPhone seized during warrant	the exe	cution of a search

Present: The Honorable	SHERI PYM, United States	SHERI PYM, United States Magistrate Judge			
Kimbe	rly I. Carter	XTR RECORDER			
Deputy Clerk		Court Reporter / Recorder			
Attorneys Present for Applicant:		Attorneys Present for Respondent:			
Tracy L. Wilkison Allen W. Chiu		Theodore J. Boutrous, Jr. Nicola T. Hanna Marc Zwillinger Bruce Sewell			
Proceedings:	Telephone Conference				

A Telephonic Conference was held in this matter on February 18, 2016. The court and counsel conferred regarding a briefing schedule on the government's anticipated motion to compel and respondent Apple Inc.'s anticipated motion for relief from the existing Order Compelling. The parties shall submit a proposed briefing schedule on February 19, 2016.

00	:	20
----	---	----

Initials of Preparer

KC

	Case 5:16-cm-00010-SP Document 9 File	d 02/19/16 Page 1 of 2 Page ID #:58	
1 2 3 4 5	THEODORE B. OLSON, SBN 38137 tolson@gibsondunn.com THEODORE J. BOUTROUS JR., SBN 1 tboutrous@gibsondunn.com NICOLA T. HANNA, SBN 130694 nhanna@gibsondunn.com ERIC D. VANDEVELDE, SBN 240699 evandevelde@gibsondunn.com GIBSON, DUNN & CRUTCHER LLP 333 South Grand Avenue	32099	
6 7	Los Angeles, CA 90071-3197 Telephone: 213.229.7000 Facsimile: 213.229.7520		
8	Attorneys for Apple Inc.		
9	UNITED STATE	S DISTRICT COURT	
10	CENTRAL DISTR	ICT OF CALIFORNIA	
11	EASTER	N DIVISION	
12	IN THE MATTER OF THE SEARCH	ED No. CM 10-16-SP	
13	OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A	SCHEDULING ORDER	
14	SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA	Hearing:	
15	LICENSE PLÁTE 35KGD203	Date: March 22, 2016 Time: 1:00 p.m.	
16		Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym	
17			
18	1. Apple Inc. ("Apple") has info	ormed the government and the Court that it	
19	will seek relief from the Court's February	16, 2016 Order Compelling Apple to Assist	
20	Agents in Search (the "Order").		
21	2. On February 18, 2016, the C	ourt held a telephonic status conference in	
22	this matter and heard the positions of the government and Apple with respect to an		
23	appropriate briefing schedule for Apple's application for relief.		
24	3. On February 19, 2016, the government filed a <i>Motion to Compel Apple</i>		
25	Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in		
26	Search.		
27			
28			
Gibson, Dunn & Crutcher LLP			

4. The Court will hear Apple's application for relief and the government's motion to compel on March 22, 2016, at 1:00 p.m., and sets the following briefing schedule:

i. Apple shall file its application for relief/opposition to the government's motion by not later than February 26, 2016;

Any amicus brief shall be filed by not later than March 3, 2016, ii. along with an appropriate request seeking leave of the Court to file such brief;

iii. The government's opposition to Apple's application for relief/reply to the government's motion shall be filed by not later than March 10, 2016; and

10 Apple shall file any reply with respect to its application for relief by iv. not later than March 15, 2016.

Apple shall have 35 pages for its application for relief/opposition to the 12 5. 13 government's motion, and the government shall have 35 pages for its opposition to Apple's application for relief/reply to the government's motion. All other filings shall 14 15 conform to the page limits set forth in the Local Rules.

16 6. The Order currently imposes a five-day deadline by which Apple must 17 seek relief from the Court. In light of the schedule set forth herein, that deadline is 18 vacated; Apple shall seek relief from the Court by February 26, 2016.

19 IT IS SO ORDERED.

102074785.1.DOC

20 Dated: February 19, 2016

Honorable Sheri Pym United States Magistrate Judge

Gibson, Dunn & Crutcher LLP

1

2

3

4

5

6

7

8

9

11

21

22

23

24

25

26

27