

1 EILEEN M. DECKER
United States Attorney
2 PATRICIA A. DONAHUE
Assistant United States Attorney
3 Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
4 Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section
5 ALLEN W. CHIU (California Bar No. 240516)
Assistant United States Attorney
6 Terrorism and Export Crimes Section
1500 United States Courthouse
7 312 North Spring Street
Los Angeles, California 90012
8 Telephone: (213) 894-0622/2435
Facsimile: (213) 894-8601
9 Email: Tracy.Wilkison@usdoj.gov
Allen.Chiu@usdoj.gov

10 Attorneys for Applicant
11 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
15 THE EXECUTION OF A SEARCH
WARRANT ON A BLACK LEXUS IS300,
16 CALIFORNIA LICENSE PLATE
35KGD203

CM 16-10
ED No. [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

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

2016 FEB 19 AM 10:06
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
BY X

FILED

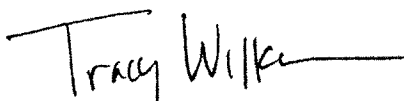
1 This Motion is based upon the attached memorandum of points and
2 authorities, the attached exhibit, the files and records in this case
3 including the application and order compelling Apple to assist the
4 FBI and the underlying search warrant, and such further evidence and
5 argument as the Court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

6
7 Dated: February 19, 2016

Respectfully submitted,

8 EILEEN M. DECKER
9 United States Attorney

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

12 

13 TRACY L. WILKISON
14 ALLEN W. CHIU
Assistant ~~United~~ States Attorneys

15 Attorneys for Applicant
16 UNITED STATES OF AMERICA
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

<u>DESCRIPTION</u>	<u>PAGE</u>
TABLE OF AUTHORITIES.....	ii
MEMORANDUM OF POINTS AND AUTHORITIES.....	1
I. INTRODUCTION.....	1
II. STATEMENT OF FACTS.....	3
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.....	7
A. This Court's All Writs Act Order is Lawful and Binding....	7
1. The All Writs Act.....	7
2. Apple is not "far removed" from this matter.....	10
3. The Order does not place an unreasonable burden on Apple.....	12
4. Apple's assistance is necessary to effectuate the warrant.....	16
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.....	18
6. Public Policy Favors Enforcing of the Order.....	21
B. Congress has Not Limited this Court's Authority to Issue an All Writs Act Order to Apple.....	21
1. No statute addresses data extraction from a passcode-locked cell phone.....	22
2. Congressional inaction does not deprive courts of their authority under the All Writs Act.....	24
IV. CONCLUSION.....	25

TABLE OF AUTHORITIES

<u>DESCRIPTION</u>	<u>PAGE</u>
<u>FEDERAL CASES</u>	
<u>Central Bank of Denver v. First Interstate Bank of Denver,</u> 511 U.S. 164 (1994).....	24
<u>General Construction Company v. Castro,</u> 401 F.3d 963 (9th Cir. 2005).....	24
<u>In re Application of the United States for an Order</u> <u>Directing a Provider of Communication Services to Provide</u> <u>Technical Assistance to the DEA, 2015 WL 5233551, at *4-5</u> <u>(D.P.R. Aug. 27, 2015).....</u>	9
<u>In re Application of United States for an Order Authorizing an</u> <u>In-Progress Trace of Wire Commc'ns over Tel. Facilities</u> <u>(Mountain Bell), 616 F.2d 1122 (9th Cir. 1980).....</u>	passim
<u>In re Application of United States for an Order Directing X to</u> <u>Provide Access to Videotapes (Access to Videotapes),</u> <u>2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003)</u> <u>(unpublished).....</u>	9, 12
<u>In re Order Requiring [XXX], Inc. to Assist in the Execution</u> <u>of a Search Warrant Issued by This Court by Unlocking a</u> <u>Cellphone (In re XXX), 2014 WL 5510865, at *2 (S.D.N.Y.</u> <u>Oct. 31, 2014).....</u>	9, 15
<u>Konop v. Hawaiian Airlines, Inc.,</u> 302 F.3d 868 (9th Cir. 2002).....	22
<u>Pennsylvania Bureau of Correction v. United States Marshals</u> <u>Service,</u> 474 U.S. 34 (1985).....	7, 22, 24
<u>Plum Creek Lumber Co. v. Hutton,</u> 608 F.2d 1283 (9th Cir. 1979).....	7
<u>Riley v. California,</u> 134 S. Ct. 2473 (2014).....	21
<u>United States v. Catoggio,</u> 698 F.3d 64 (2d Cir. 2012).....	8
<u>United States v. Craft,</u> 535 U.S. 274 (2002).....	24
<u>United States v. Fricosu,</u> 841 F.Supp.2d 1232 (D. Co. 2012).....	17

1	<u>United States v. Hall,</u>	
2	583 F. Supp. 717 (E.D. Va. 1984).....	9, 12
3	<u>United States v. Li,</u>	
4	55 F.3d 325, 329 (7th Cir. 1995).....	15
5	<u>United States v. Navarro,</u>	
6	No. 13-CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013).....	9
7	<u>United States v. New York Telephone Co.,</u>	
8	434 U.S. 159 (1977).....	<i>passim</i>

FEDERAL STATUTES

9	18 U.S.C. § 2510.....	22
10	18 U.S.C. § 3103.....	21
11	28 U.S.C. § 1651.....	7
12	47 U.S.C. § 1001.....	22
13	47 U.S.C. § 1002.....	22, 23

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.

1 Apple left the government with no option other than to apply to
2 this Court for the Order issued on February 16, 2016. The Order
3 requires Apple to assist the FBI with respect to this single iPhone
4 used by Farook by providing the FBI with the opportunity to determine
5 the passcode. The Order does not, as Apple's public statement
6 alleges, require Apple to create or provide a "back door" to every
7 iPhone; it does not provide "hackers and criminals" access to
8 iPhones; it does not require Apple to "hack [its] own users" or to
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
11 authorization; and it does not compromise the security of personal
12 information. See Exhibit 1. To the contrary, the Order allows Apple
13 to retain custody of its software at all times, and it gives Apple
14 flexibility in the manner in which it provides assistance. In fact,
15 the software never has to come into the government's custody.

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

24 ¹ Apple's Legal Process Guidelines continue to state that Apple
25 will provide assistance with unlocking devices running iOS versions
26 earlier than 8.0, and advises as to what language to include in the
27 order. See "Extracting Data from Passcode Locked iOS Devices," Apple
28 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.

1 appears to be based on its concern for its business model and public
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
5 believes that compliance with this Order would be unreasonably
6 burdensome, it may make an application to this Court for relief
7 within five business days of receipt of the Order," Apple's public
8 statement makes clear that Apple will not comply with the Court's
9 Order. The government does not seek to deny Apple its right to be
10 heard, and expects these issues to be fully briefed before the Court;
11 however, the urgency of this investigation requires this motion now
12 that Apple has made its intention not to comply patently clear.³
13 This aspect of the investigation into the December 2, 2015 terrorist
14 attack must move forward.

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
18 ("SSA") Christopher Pluhar, which was attached thereto, both of which
19 were filed on February 16, 2016, the FBI has been investigating the

20 ² As Apple has stated on its web page, "Our commitment to
21 customer privacy doesn't stop because of a government information
22 request. ... Unlike our competitors, Apple cannot bypass your passcode
23 and therefore cannot access this data. So it's not technically
24 feasible for us to respond to government warrants for the extraction
25 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.

26 ³ Although a separate order compelling Apple's compliance with
27 this Court's February 16, 2016, order is not legally necessary, in
28 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.

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

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

23 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

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

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

22 The information and data contained on the SUBJECT DEVICE is of
23 particular concern to the government because, while evidence found on
24 the iCloud account associated with the SUBJECT DEVICE indicates that
25 Farook communicated with victims who were later killed during the
26

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

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

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

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

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

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

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

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

17 1. The All Writs Act

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

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

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

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

9 Further, based on the authority given under the All Writs Act,
10 courts have issued orders, similar to the one the Court issued here,
11 that require a manufacturer to attempt to assist in accessing a
12 cellphone's image files so that a warrant may be executed as
13 originally contemplated. See, e.g., In re Order Requiring [XXX],
14 Inc. to Assist in the Execution of a Search Warrant Issued by This
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-
17 CR-5525, ECF No. 39 (W.D. Wa. Nov. 13, 2013). Courts have also
18 issued All Writs Act orders in support of warrants in a wide variety
19 of contexts, including ordering a phone company to assist with a trap
20 and trace device (Mountain Bell, 616 F.2d at 1129); ordering a credit
21 card company to produce customer records (United States v. Hall, 583
22 F. Supp. 717, 722 (E.D. Va. 1984)); ordering a landlord to provide
23 access to security camera videotapes (In re Application of United
24 States for an Order Directing X to Provide Access to Videotapes
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
28 United States for an Order Directing a Provider of Communication

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

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

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

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

24 ⁵ In litigation pending before a Magistrate Judge in the Eastern
25 District of New York, that court sua sponte raised the issue of
26 whether it had authority under the All Writs Act to issue a similar
27 order. That out-of-district litigation remains pending without any
28 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.

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

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

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

21 Moreover, other courts have directed All Writs Act orders based
22 on warrants to entities that are not public utilities. For example,
23 neither the credit card company in Hall nor the landlord in Access to
24 Videotapes was a public utility. See Hall, 583 F. Supp. at 722;
25 Access to Videotapes, 2003 WL 22053105, at *3. Apple's close
26 relationship to the iPhone and its software, both legally and
27 technically – which are the produce of Apple's own design – makes
28

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

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

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

19 While the Order in this case requires Apple to provide or employ
20 modified software, modifying an operating system - which is
21 essentially writing software code in discrete and limited manner - is
22 not an unreasonable burden for a company that writes software code as
23 part of its regular business.⁶ The simple fact of having to create
24 code that may not now exist in the exact form required does not an
25 undue burden make. In fact, providers of electronic communications
26

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

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

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

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

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

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

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

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

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

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

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

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

17 Moreover, as discussed above, Apple's assistance is necessary
18 because without the access to Apple's software code and ability to
19 cryptographically sign code for the SUBJECT DEVICE that only Apple
20 has, the FBI cannot attempt to determine the passcode without fear of
21 permanent loss of access to the data or excessive time delay.

22 Indeed, after reviewing a number of other suggestions to obtain the
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
25 methods - besides that which is now ordered by this Court - that are
26 feasible for gaining access to the currently inaccessible data on the
27
28

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

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

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

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

18 ⁷ The four suggestions that Apple and the FBI discussed (and
 19 their deficiencies) were: (1) to obtain cell phone toll records for
 20 the SUBJECT DEVICE (which, while the government has of course done
 21 so, is insufficient because there is far more information on the
 22 SUBJECT DEVICE than simply toll records); (2) to determine if any
 23 computers were paired with the SUBJECT DEVICE to obtain data (which
 24 the government has determined that none were); (3) to attempt an
 25 auto-backup of the SUBJECT DEVICE with the related iCloud account
 26 (which would not work in this case because neither the owner nor the
 27 government knew the password to the iCloud account, and the owner, in
 28 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.

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

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

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

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

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

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

8 6. Public Policy Favors Enforcing of the Order

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

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

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

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

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

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

19 In particular, neither Federal Rule of Criminal Procedure 41 nor
 20 the Communications Assistance for Law Enforcement Act ("CALEA"), 47
 21 U.S.C. § 1002, "specifically addresses" – or even vaguely addresses –
 22 the duty of Apple to assist in extracting data from a passcode-locked
 23 cell phone in order to permit the government to execute a validly
 24 issued search warrant. CALEA requires telecommunications carriers to
 25 retain the capability to comply with court orders for real-time
 26 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)

1 Id. By contrast, this case involves evidence already stored on a
 2 cell phone (data "at rest"). Here, Apple is not acting as a
 3 telecommunications carrier, and the Order concerns access to stored
 4 data rather than real-time interceptions and call-identifying
 5 information. Put simply, CALEA is entirely inapplicable to the
 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
 8 a search warrant.⁹

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

19 _____
 20 and electronic communications carried by the carrier. 47 U.S.C.
 21 § 1002(a)(1). CALEA incorporates the definition of "intercept" from
 22 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).

23 ⁹ Furthermore, nothing in CALEA prevents a court from ordering a
 24 telecommunications carrier to decrypt communications that the carrier
 25 is capable of decrypting. See 47 U.S.C. § 1002(b)(3). When Congress
 26 enacted CALEA, it understood that existing provider-assistance
 27 provisions required a provider to decrypt communications when it was
 28 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).

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

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

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

18 The Supreme Court and the Ninth Circuit have repeatedly
19 cautioned that "Congressional inaction lacks persuasive significance
20 because several equally tenable inferences may be drawn from such
21 inaction[.]" General Construction Company v. Castro, 401 F.3d 963,
22 970-71 (9th Cir. 2005) (quoting Central Bank of Denver v. First
23 Interstate Bank of Denver, 511 U.S. 164, 187 (1994)); see also United
24 States v. Craft, 535 U.S. 274, 287 (2002).

25 Here, there are many possible explanations for congressional
26 inaction on encryption, including that Congress is satisfied with
27 existing authorities, or that Congress has not yet reached agreement
28 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

Shop and Learn

Mac
iPad
iPhone
Watch
TV
Music
iTunes
iPod
Accessories
Gift Cards

Apple Store

Find a Store
Genius Bar
Workshops and Learning
Youth Programs
Apple Store App
Refurbished
Financing
Reuse and Recycling
Order Status
Shopping Help

For Education

Apple and Education
Shop for College

For Business

iPhone in Business
iPad in Business
Mac in Business
Shop for Your Business

Account

Manage Your Apple ID
Apple Store Account
iCloud.com

Apple Values

Environment
Supplier Responsibility
Accessibility
Privacy
Inclusion and Diversity
Education

About Apple

Apple Info
Job Opportunities
Press Info
Investors
Events
Hot News
Legal
Contact Apple

More ways to shop: visit a Apple Store, call 1-800-MY-APPLE, or find a reseller

Copyright © 2016 Apple Inc. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Sales and Refunds](#) [Site Map](#)

United States

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. Vandeveld Gibson, Dunn & Crutcher LLP evandeveld@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