

1 THEODORE J. BOUTROUS JR., SBN 132099
tboutrous@gibsondunn.com
2 NICOLA T. HANNA, SBN 130694
nhanna@gibsondunn.com
3 ERIC D. VANDEVELDE, SBN 240699
evandeveld@ibsondunn.com
4 GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
5 Los Angeles, CA 90071-3197
Telephone: 213.229.7000
6 Facsimile: 213.229.7520

7 THEODORE B. OLSON, SBN 38137
tolson@gibsondunn.com
8 GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
9 Washington, DC, 20036-5306
Telephone: 202.955.8500
10 Facsimile: 202.467.0539

11 MARC J. ZWILLINGER*
marc@zwillgen.com
12 JEFFFREY G. LANDIS*
jeff@zwillgen.com
13 ZWILLGEN PLLC
1900 M Street N.W., Suite 250
14 Washington, D.C. 20036
Telephone: 202.706.5202
15 Facsimile: 202.706.5298
*Pro Hac Vice Admission Pending

16 Attorneys for Apple Inc.

17 UNITED STATES DISTRICT COURT
18 CENTRAL DISTRICT OF CALIFORNIA
19 EASTERN DIVISION

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

ED No. CM 16-10 (SP)

**APPLE INC'S MOTION TO VACATE
ORDER COMPELLING APPLE INC.
TO ASSIST AGENTS IN SEARCH,
AND OPPOSITION TO
GOVERNMENT'S MOTION TO
COMPEL ASSISTANCE**

Hearing:

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

1 Apple Inc. (“Apple”), by and through its counsel of record, hereby files this
2 Motion to Vacate the Order Compelling Apple Inc. to Assist Agents in Search, and
3 Opposition to the Government’s Motion to Compel Assistance.

4 This Motion and Opposition is based upon the attached memorandum of points
5 and authorities, the attached declarations of Nicola T. Hanna, Lisa Olle, and Erik
6 Neuenschwander and exhibits, the files and records in this case, and such further
7 evidence and argument as the Court may permit.

8
9 Dated: February 25, 2016

Respectfully submitted,

10 GIBSON, DUNN & CRUTCHER LLP

11 By: /s/ Theodore J. Boutrous, Jr.
12 Theodore J. Boutrous, Jr.

13 Theodore J. Boutrous, Jr.
14 Nicola T. Hanna
15 Eric D. Vandavelde
16 Gibson, Dunn & Crutcher LLP
17 333 South Grand Avenue
18 Los Angeles, CA 90071-3197
19 Telephone: 213.229.7000
20 Facsimile: 213.229.7520

21 Theodore B. Olson
22 Gibson, Dunn & Crutcher LLP
23 1050 Connecticut Avenue, N.W.
24 Washington, DC, 20036-5306
25 Telephone: 202.955.8500
26 Facsimile: 202.467.0539

27 Marc J. Zwillinger *
28 Jeffrey G. Landis *
ZwillGen PLLC
1900 M Street N.W., Suite 250
Washington, D.C. 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298
**Pro Hac Vice Admission Pending*

Attorneys for Apple Inc.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. BACKGROUND	5
A. Apple’s Industry-Leading Device Security.....	5
B. The Government Abandoned Efforts To Obtain Legal Authority For Mandated Back Doors.	6
C. Apple’s Substantial Assistance In The Government’s Investigation.....	100
D. The Government’s <i>Ex Parte</i> Application Under The All Writs Act, And This Court’s Order	111
E. The Resources And Effort Required To Develop The Software Demanded By The Government	13
III. ARGUMENT.....	144
A. The All Writs Act Does Not Provide A Basis To Conscript Apple To Create Software Enabling The Government To Hack Into iPhones.	144
1. The All Writs Act Does Not Grant Authority To Compel Assistance Where Congress Has Considered But Chosen Not To Confer Such Authority.	15
2. <i>New York Telephone Co.</i> And Its Progeny Confirm That The All Writs Act Does Not Authorize Courts To Compel The Unprecedented And Unreasonably Burdensome Conscription Of Apple That The Government Seeks.....	20
a. Apple’s Connection To The Underlying Case Is “Far Removed” And Too Attenuated To Compel Its Assistance	200
b. The Order Requested By The Government Would Impose An Unprecedented And Oppressive Burden On Apple And Citizens Who Use The iPhone.....	23
c. The Government Has Not Demonstrated Apple’s Assistance Was Necessary To Effectuating The Warrant.	29
3. Other Cases The Government Cites Do Not Support The Type Of Compelled Action Sought Here.	300
B. The Order Would Violate The First Amendment And The Fifth Amendment’s Due Process Clause.	322
1. The First Amendment Prohibits The Government From Compelling Apple To Create Code	322

TABLE OF CONTENTS
(Continued)

	2.	The Fifth Amendment’s Due Process Clause Prohibits The Government From Compelling Apple To Create The Request Code	<u>Page</u> 344
IV.	CONCLUSION		355

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

Page(s)

Cases

1

2

3

4 *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*,
 307 F. Supp. 2d 1085 (N.D. Cal. 2004)..... 32

5

6 *Alzheimer’s Inst. of Am. Inc. v. Elan Corp.*,
 2013 WL 8744216 (N.D. Cal. Jan. 31, 2013)..... 18

7 *In the Matter of an Application of U.S. of Am. for an Order Authorizing*
8 *Disclosure of Location Info. of a Specified Wireless Tel.*,
 849 F. Supp. 2d 526 (D. Md. 2011)..... 15

9

10 *Application of U.S. of Am. for an Order Authorizing an In-Progress Trace*
 of Wire Commc’ns over Tel. Facilities, 616 F.2d 1122 21, 22, 27, 29

11

12 *In re Application of U.S. of Am. for an Order Directing a Provider of*
13 *Commc’n Servs. to Provide Tech. Assistance to Agents of the U.S.*
 Drug Enf’t Admin.,
14 2015 WL 5233551 (D.P.R. Aug. 27, 2015)..... 27

15 *In re Application of U.S. of Am. for an Order Directing X to Provide*
16 *Access to Videotapes (“Videotapes”)*,
 2003 WL 22053105 (D. Md. Aug. 22, 2003)..... 21, 27

17

18 *Ayres v. Ocwen Loan Serv., LLC*,
 2013 WL 4784190 (D. Md. Sept. 5, 2013)..... 5

19

20 *Baker v. Carr*,
 369 U.S. 186 (1962)..... 19

21

22 *Bernstein v. Dep’t of State*,
 922 F. Supp. 1426 (N.D. Cal. 1996)..... 32

23

24 *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*,
 511 U.S. 164 (1994)..... 18

25

26 *Clark v. Martinez*,
 543 U.S. 371 (2005)..... 18

27

28 *Clinton v. Jones*,
 520 U.S. 681 (1997)..... 18

TABLE OF AUTHORITIES
(Continued)

Page(s)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Cnty. of Sacramento v. Lewis,
523 U.S. 833 (1998)..... 34

Costanich v. Dep’t of Soc. & Health Servs.,
627 F.3d 1101 (9th Cir. 2010) 34

Diamond v. Chakrabarty,
447 U.S. 303 (1980)..... 19

Douglas Oil Co. of Cal. v. Petrol Stops Nw.,
441 U.S. 211 (1979)..... 33

Grannis v. Ordean,
234 U.S. 385 (1914)..... 11

Junger v. Daley,
209 F.3d 481 (6th Cir. 2000) 32

Members of City Council v. Taxpayers for Vincent,
466 U.S. 789 (1984)..... 34

Mich. Bell Telephone Co. v. United States,
565 F.2d 385 (6th Cir. 1977) 29

Mullane v. Cent. Hanover Bank & Tr. Co.,
339 U.S. 306 (1950)..... 11

In re Order,
2015 WL 5920207 16, 19, 22

*In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search
Warrant Issued by This Court by Unlocking a Cellphone*,
2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014) (“*Order Requiring
[XXX]*”) 28

*In re Order Requiring Apple Inc. to Assist in the Execution of a Search
Warrant Issued by the Court*,
E.D.N.Y No. 15 MC 1902, Dkt. 19 22

*In re Order Requiring Apple, Inc. to Assist in the Execution of a Search
Warrant Issued by this Court*,
E.D.N.Y No. 15-MC-1902, Dkt. 27 3

TABLE OF AUTHORITIES
(Continued)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

	<u>Page(s)</u>
<i>Pa. Bureau of Corr. v. U.S. Marshals Serv.</i> , 474 U.S. 34 (1985).....	15
<i>Pipe Trades Council, U.A. Loc. 159 v. Underground Contractors Ass’n</i> , 835 F.2d 1275 (9th Cir. 1987)	5
<i>Plaut v. Spendthrift Farm, Inc.</i> , 514 U.S. 211 (1995).....	18
<i>Plum Creek Lumber Co. v. Hutton</i> , 608 F.2d 1283 (9th Cir. 1979)	1, 14, 15, 31, 32
<i>Quon v. Arch Wireless Operating Co., Inc.</i> , 529 F.3d 892 (9th Cir. 2008)	17
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	25
<i>Riley v. Nat’l Fed. of the Blind of N.C., Inc.</i> , 487 U.S. 781,796 (1988).....	32
<i>Saldana v. Occidental Petroleum Corp.</i> , 774 F.3d 544 (9th Cir. 2014) (per curiam)	19
<i>In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203</i> , No. ED 15-0451M (Feb. 16, 2016), Dkt.	12, 22, 31
<i>State v. Underdahl</i> , 767 N.W.2d 677 (Minn. 2009)	24
<i>Turner Broad. Sys., Inc. v. FCC</i> , 512 U.S. 622 (1994).....	33
<i>United States v. Budziak</i> , 697 F.3d 1105 (9th Cir. 2012)	24
<i>United States v. Cameron</i> , 699 F.3d 621 (1st Cir. 2012).....	26
<i>United States v. Catoggio</i> , 698 F.3d 64 (2d Cir. 2012) (per curiam)	30

TABLE OF AUTHORITIES
(Continued)

Page(s)

1

2 *United States v. Cooper*,

3 983 F.2d 928 (9th Cir. 1993) 24

4 *United States v. Elcom Ltd.*,

5 203 F. Supp. 2d 1111 (N.D. Cal. 2002)..... 32

6 *United States v. Fricosu*,

7 841 F. Supp. 2d 1232 (D. Colo. 2012) 30

8 *United States v. Hall*,

9 583 F. Supp. 717 (E.D. Va. 1984) 21, 23, 27

10 *United States v. Navarro*,

11 No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39..... 28

12 *United States v. New York Telephone Co.*,

13 434 U.S. 159 (1977)..... 20, 21, 22, 29, 30

14 *Universal City Studios, Inc. v. Corley*,

15 273 F.3d 429 (2d Cir. 2001) 32

16 *Vieth v. Jubelirer*,

17 541 U.S. 267 (2004) (plurality opinion) 19

18 *Xi v. INS*,

19 298 F.3d 832 (9th Cir. 2002) 19

20 *Youngstown Sheet & Tube Co. v. Sawyer*,

21 343 U.S. 579 (1952)..... 18

Statutes

22 18 U.S.C. § 2518(4) 17

23 18 U.S.C. § 3282 35

24 28 U.S.C. § 1651 11, 15, 19

25 47 U.S.C. § 1001 8, 17

26 47 U.S.C. § 1002 8, 16, 17

27

28

TABLE OF AUTHORITIES
(Continued)

Page(s)

Other Authorities

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Apple Inc., <i>A Message to Our Customers</i> (Feb. 16, 2016)	3, 22
Apple Inc. and Apple Distrib. Int’l, Written Evidence (IPB0093), (Dec. 21, 2015)	7
Apple Inc., <i>iCloud: Back up your iOS device to iCloud</i>	11
Apple Inc., <i>iOS Security: iOS 9.0 or later</i> (September 2015).....	6
Apple Inc., <i>Privacy, Government Information Requests</i>	33
Comey, <i>Follow This Lead</i>	4, 12, 33
Comey, <i>Going Dark</i>	4, 12
Cyrus R. Vance Jr., <i>No Smartphone Lies Beyond the Reach of a Judicial Search Warrant</i> , N.Y. Times (Feb. 18, 2016).....	10, 24
Damian Paletta, <i>How the U.S. Fights Encryption—and Also Helps Develop It</i> , Wall St. J. (Feb. 22, 2016)	6
Ellen Nakashima, <i>Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say</i> , Wash. Post (July 9, 2015)	1
Ellen Nakashima and Mark Berman, <i>FBI Asked San Bernardino to Reset the Password for Shooter’s Phone Backup</i> , Wash. Post (Feb. 20, 2016)	34
Ellen Nakashima, <i>Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders</i> , Wash. Post (Apr. 28, 2013).....	9
FBI, Operational Technology, <i>Going Dark Issue</i> (last visited Feb. 23, 2016)	4, 7
Gen. Michael Hayden <i>Gives an Update on the Cyberwar</i> , Wall St. J. (Feb. 17, 2016)	5
H.R. 2233, 114th Cong. (2015) (same, adding additional amendments to the Foreign Intelligence Surveillance Act of 1978)	9
H.R. Rep. No. 103-827(I), (1994)	8, 17

TABLE OF AUTHORITIES
(Continued)

Page(s)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

James Comey, *Director Discusses Encryption, Patriot Act Provisions* (May 20, 2015) 10

James Comey, *Encryption, Public Safety, and “Going Dark,”* 4

James Comey, “Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption,” Joint Statement with Deputy Atty Gen. Sally Quillian Yates Before the Sen. Judiciary Comm. (July 8, 2015) 7

James Comey, *Statement Before the Senate Comm. on Homeland Sec. & Governmental Affairs* (Oct. 8, 2015) 9

James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead* 4

Kara Swisher, *White House. Red Chair. Obama Meets Swisher* (Feb. 15, 2015) 10

Margaret Coker, et al., *The Attacks in Paris: Islamic State Teaches Tech Savvy*, Wall St. J. (Nov. 17, 2015) 4

Mike McConnell et al., *Why The Fear Over Ubiquitous Data Encryption Is Overblown*, Wash. Post (July 28, 2015) 8

New America’s Open Technology Institute, *Joint Letter to President Barack Obama* (May 19, 2015) 9

NPR, Weekend Edition, *It’s Not Just the iPhone Law Enforcement Wants to Unlock* (Feb. 21, 2016) 10

Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference (Jan. 16, 2015) 10

Secure Data Act of 2015, H.R. 726, 114th Cong. (2015) 9

Secure Data Act of 2015, S.135, 114th Cong. (2015) 9

Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption, House Comm. on the Judiciary, Democrats (Feb. 18, 2016) 9

TABLE OF AUTHORITIES
(Continued)

Page(s)

Seung Lee, *The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories*, Newsweek (Feb. 19, 2016) 3

Susan Landau, *The National-Security Needs for Ubiquitous Encryption* (Feb. 1, 2016)..... 7

Rules

Fed. R. Evid. 404 35

Fed. R. Evid. 702 24

Constitutional Provisions

U.S. Const. amend. IV 35

1 MEMORANDUM OF POINTS AND AUTHORITIES

2 I. INTRODUCTION

3 This is not a case about one isolated iPhone. Rather, this case is about the
4 Department of Justice and the FBI seeking through the courts a dangerous power that
5 Congress and the American people have withheld: the ability to force companies like
6 Apple to undermine the basic security and privacy interests of hundreds of millions of
7 individuals around the globe. The government demands that Apple create a back door
8 to defeat the encryption on the iPhone, making its users' most confidential and
9 personal information vulnerable to hackers, identity thieves, hostile foreign agents, and
10 unwarranted government surveillance. The All Writs Act, first enacted in 1789 and on
11 which the government bases its entire case, "does not give the district court a roving
12 commission" to conscript and commandeer Apple in this manner. *Plum Creek Lumber*
13 *Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979). In fact, no court has ever
14 authorized what the government now seeks, no law supports such unlimited and
15 sweeping use of the judicial process, and the Constitution forbids it.

16 Since the dawn of the computer age, there have been malicious people dedicated
17 to breaching security and stealing stored personal information. Indeed, the government
18 itself falls victim to hackers, cyber-criminals, and foreign agents on a regular basis,
19 most famously when foreign hackers breached Office of Personnel Management
20 databases and gained access to personnel records, affecting over 22 million current and
21 former federal workers and family members.¹ In the face of this daily siege, Apple is
22 dedicated to enhancing the security of its devices, so that when customers use an
23 iPhone, they can feel confident that their most private personal information—financial
24 records and credit card information, health information, location data, calendars,
25 personal and political beliefs, family photographs, information about their children—

26 _____
27 ¹ See, e.g., Hanna Decl. Ex. A [Ellen Nakashima, *Hacks of OPM Databases*
28 *Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (July 9,
2015)] (explaining that hackers used stolen logins and passwords to gain access to
federal employee records databases for six months before detection).

1 will be safe and secure. To this end, Apple uses encryption to protect its customers
2 from cyber-attack and works hard to improve security with every software release
3 because the threats are becoming more frequent and sophisticated. Beginning with
4 iOS 8, Apple added additional security features that incorporate the passcode into the
5 encryption system. It is these protections that the government now seeks to roll back
6 by judicial decree.

7 There are two important and legitimate interests in this case: the needs of law
8 enforcement and the privacy and personal safety interests of the public. In furtherance
9 of its law enforcement interests, the government had the opportunity to seek
10 amendments to existing law, to ask Congress to adopt the position it urges here. But
11 rather than pursue new legislation, the government backed away from Congress and
12 turned to the courts, a forum ill-suited to address the myriad competing interests,
13 potential ramifications, and unintended consequences presented by the government's
14 unprecedented demand. And more importantly, by invoking "terrorism" and moving
15 *ex parte* behind closed courtroom doors, the government sought to cut off debate and
16 circumvent thoughtful analysis.

17 The order demanded by the government compels Apple to create a new
18 operating system—effectively a "back door" to the iPhone—that Apple believes is too
19 dangerous to build. Specifically, the government would force Apple to create new
20 software with functions to remove security features and add a new capability to the
21 operating system to attack iPhone encryption, allowing a passcode to be input
22 electronically. This would make it easier to unlock the iPhone by "brute force," trying
23 thousands or millions of passcode combinations with the speed of a modern computer.
24 In short, the government wants to compel Apple to create a crippled and insecure
25 product. Once the process is created, it provides an avenue for criminals and foreign
26 agents to access millions of iPhones. And once developed for our government, it is
27 only a matter of time before foreign governments demand the same tool.

1 The government says: “Just this once” and “Just this phone.” But the
2 government knows those statements are not true; indeed the government has filed
3 multiple other applications for similar orders, some of which are pending in other
4 courts.² And as news of this Court’s order broke last week, state and local officials
5 publicly declared their intent to use the proposed operating system to open hundreds of
6 other seized devices—in cases having nothing to do with terrorism.³ If this order is
7 permitted to stand, it will only be a matter of days before some other prosecutor, in
8 some other important case, before some other judge, seeks a similar order using this
9 case as precedent. Once the floodgates open, they cannot be closed, and the device
10 security that Apple has worked so tirelessly to achieve will be unwound without so
11 much as a congressional vote. As Tim Cook, Apple’s CEO, recently noted: “Once
12 created, the technique could be used over and over again, on any number of devices.
13 In the physical world, it would be the equivalent of a master key, capable of opening
14 hundreds of millions of locks—from restaurants and banks to stores and homes. No
15 reasonable person would find that acceptable.” Declaration of Nicola T. Hanna
16 (“Hanna Decl.”), Ex. D [Apple Inc., *A Message to Our Customers* (Feb. 16, 2016)].

17 Despite the context of this particular action, no legal principle would limit the
18 use of this technology to domestic terrorism cases—but even if such limitations could
19 be imposed, it would only drive our adversaries further underground, using encryption
20 technology made by foreign companies that cannot be conscripted into U.S.

22 ² Hanna Decl. Ex. B [Letter to Court, *In re Order Requiring Apple, Inc. to Assist in*
23 *the Execution of a Search Warrant Issued by this Court*, E.D.N.Y No. 15-MC-1902,
Dkt. 27].

24 ³ *E.g.*, Hanna Decl. Ex. C [Seung Lee, *The Murder Victim Whose Phone Couldn’t Be*
25 *Cracked and Other Apple Encryption Stories*, Newsweek (Feb. 19, 2016)] (Cyrus
26 Vance, Manhattan District Attorney stating that he has “155 to 160” devices that he
27 would like to access, while officials in Sacramento have “well over 100” devices
28 for which they would like Apple to produce unique software so that they can access
the devices’ contents); Hanna Decl. ¶ 5 at 18:28 [Charlie Rose, Television
Interview of Cyrus Vance (Feb. 18, 2016)] (Vance stating “absolutely” that he
“want[s] access to all those phones that [he thinks] are crucial in a criminal
proceeding”).

1 government service⁴—leaving law-abiding individuals shouldering all of the burdens
2 on liberty, without any offsetting benefit to public safety. Indeed, the FBI’s repeated
3 warnings that criminals and terrorists are able to “go dark” behind end-to-end
4 encryption methods proves this very point. *See* Hanna Decl. Ex. F [FBI, Operational
5 Technology, *Going Dark Issue* (last visited Feb. 23, 2016) (“FBI, Going Dark”)].

6 Finally, given the government’s boundless interpretation of the All Writs Act, it
7 is hard to conceive of any limits on the orders the government could obtain in the
8 future. For example, if Apple can be forced to write code in this case to bypass
9 security features and create new accessibility, what is to stop the government from
10 demanding that Apple write code to turn on the microphone in aid of government
11 surveillance, activate the video camera, surreptitiously record conversations, or turn on
12 location services to track the phone’s user? Nothing.

13 As FBI Director James Comey expressly recognized:

14 Democracies resolve such tensions through robust debate. . . . It may be
15 that, as a people, we decide the benefits [of strong encryption] outweigh
16 the costs and that there is no sensible, technically feasible way to optimize
17 privacy and safety in this particular context, or that public safety folks
18 will be able to do their job well enough in the world of universal strong
19 encryption. Those are decisions Americans should make, but I think part
20 of my job is [to] make sure the debate is informed by a reasonable
21 understanding of the costs.

22 Hanna Decl. Ex. G [James Comey, *Encryption, Public Safety, and “Going Dark,”*
23 *Lawfare* (July 6, 2015, 10:38 AM) (“Comey, *Going Dark*”)]; *see also* Hanna Decl. Ex.
24 H [James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow*
25 *This Lead*, *Lawfare* (Feb. 21, 2016, 9:03 PM) (“Comey, *Follow This Lead*”)]
26 (reiterating that the tension between national security and individual safety and privacy
27 “should not be resolved by the FBI, which investigates for a living[, but rather] . . . by
28 the American people . . .”). The government, by seeking an order mandating that

26 ⁴ *See* Hanna Decl. Ex. E [Margaret Coker, et al., *The Attacks in Paris: Islamic State*
27 *Teaches Tech Savvy*, *Wall St. J.* (Nov. 17, 2015) (“Coker, *Tech Savvy*”)]
28 (describing the technological sophistication of terrorists groups, including, for
example, ISIS’s ability and willingness to shift to more secure communication
methods).

1 Apple create software to destabilize the security of the iPhone and the law-abiding
2 citizens who use it to store data touching on every facet of their private lives, is not
3 acting to inform or contribute to the debate; it is seeking to avoid it.

4 Apple strongly supports, and will continue to support, the efforts of law
5 enforcement in pursuing justice against terrorists and other criminals—just as it has in
6 this case and many others. But the unprecedented order requested by the government
7 finds no support in the law and would violate the Constitution. Such an order would
8 inflict significant harm—to civil liberties, society, and national security—and would
9 preempt decisions that should be left to the will of the people through laws passed by
10 Congress and signed by the President. Accordingly, the Court should vacate the order
11 and deny the government’s motion to compel.⁵

12 II. BACKGROUND

13 A. Apple’s Industry-Leading Device Security.

14 Apple is committed to data security. Encryption provides Apple with the
15 strongest means available to ensure the safety and privacy of its customers against
16 threats known and unknown.⁶ For several years, iPhones have featured hardware- and

17 ⁵ The government filed its motion to compel notwithstanding the Court allowing an
18 eight-day period within which Apple could challenge the order compelling
19 assistance, Apple’s express indication during the parties’ February 18 status
20 conference that it intended to seek relief from the order, the Court’s entry of a
21 briefing schedule to permit the parties to address the validity of the order, and the
22 Court’s own skepticism about the utility of such a motion. That skepticism proved
23 warranted. Only three pages into the government’s 25-page motion, it concedes the
24 motion is “not legally necessary.” Dkt. 1 at 3 n.3. Nor could the government claim
25 otherwise, as the motion—substantial portions of which appear to have been cut
26 and pasted from the government’s *ex parte* application—seeks no relief beyond that
27 contemplated by the order compelling assistance. Because the government’s
28 motion serves no legal purpose, and the issues it raises will be fully briefed and
addressed in Apple’s motion to vacate and the government’s opposition thereto, it
should be denied. *See, e.g., Pipe Trades Council, U.A. Loc. 159 v. Underground
Contractors Ass’n*, 835 F.2d 1275, 1279 (9th Cir. 1987) (concluding a district court
properly denied a motion to compel as premature); *cf. Ayres v. Ocwen Loan Serv.,
LLC*, 2013 WL 4784190, at *3 (D. Md. Sept. 5, 2013) (striking *sua sponte* a motion
that was “not technically ripe” and “meandering, redundant, transparent, and largely
oblivious to the posture of the case”).

⁶ Former NSA and CIA Director Michael Hayden has recognized that, on balance,
America is more secure because of “end-to-end unbreakable encryption.” Hanna
Decl. Ex. I [*Gen. Michael Hayden Gives an Update on the Cyberwar*, Wall St. J.

(*Cont'd on next page*)

1 software-based encryption of their password-protected contents. Declaration of Erik
2 Neuenschwander (“Neuenschwander Decl.”) ¶ 8. These protections safeguard the
3 encryption keys on the device with a passcode designated by the user during setup. *Id.*
4 ¶ 9. This passcode immediately becomes entangled with the iPhone’s Unique ID
5 (“UID”), which is permanently assigned to that one device during the manufacturing
6 process. *Id.* ¶ 13. The iPhone’s UID is neither accessible to other parts of the
7 operating system nor known to Apple. *See generally* Hanna Decl. Ex. K [Apple Inc.,
8 *iOS Security: iOS 9.0 or later* (September 2015)]. These protections are designed to
9 prevent anyone without the passcode from accessing encrypted data on iPhones.
10 Neuenschwander Decl. ¶ 8 .

11 Cyber-attackers intent on gaining unauthorized access to a device could break a
12 user-created passcode, if given enough chances to guess and the ability to test
13 passwords rapidly by automated means. To prevent such “brute-force” attempts to
14 determine the passcode, iPhones running iOS 8 and higher include a variety of
15 safeguards. *Id.* ¶ 10. For one, Apple uses a “large iteration count” to slow attempts to
16 access an iPhone, ensuring that it would take years to try all combinations of a six-
17 character alphanumeric passcode. *Id.* ¶ 11. In addition, Apple imposes escalating time
18 delays after the entry of each invalid passcode. *Id.* ¶ 12. Finally, Apple also includes a
19 setting that—if activated—automatically deletes encrypted data after ten consecutive
20 incorrect attempts to enter the passcode. *Id.* This combination of security features
21 protects users from attackers or if, for example, the user loses the device.

22 **B. The Government Abandoned Efforts To Obtain Legal Authority For**
23 **Mandated Back Doors.**

24 Some in the law enforcement community have disparaged the security
25 improvements by Apple and others, describing them as creating a “going dark”

26

(Cont'd from previous page)

27 (Feb. 17, 2016)]; *cf.* Hanna Decl. Ex. J [Damian Paletta, *How the U.S. Fights*
28 *Encryption—and Also Helps Develop It*, Wall St. J. (Feb. 22, 2016)] (describing
funding by U.S. government of stronger encryption technologies).

1 problem in which law enforcement may possess the “legal authority to intercept and
2 access communications and information pursuant to court orders” but lack the
3 “technical ability to carry out those orders because of a fundamental shift in
4 communications services and technologies.”⁷ As a result, some officials have
5 advanced the view that companies should be required to maintain access to user
6 communications and data and provide that information to law enforcement upon
7 satisfaction of applicable legal requirements.⁸ This would give the government, in
8 effect, a back door to otherwise encrypted communications—which would be precisely
9 the result of the government’s position in this case.⁹

10 Apple and other technology companies, supported by leading security experts,
11 have disagreed with law enforcement’s position, observing that any back door enabling
12 government officials to obtain encrypted data would also create a vulnerability that
13 could be exploited by criminals and foreign agents, weakening critical security
14 protections and creating new and unforeseen access to private information. For these
15 reasons, Apple and others have strongly opposed efforts to require companies to enable
16 the government to obtain encrypted information, arguing that this would compromise
17 the security offered to its hundreds of millions of law-abiding customers in order to
18 weaken security for the few who may pose a threat.¹⁰

19 As leading former national security officials have made clear, Apple’s
20 “resistance to building in a back door” in whatever form it may take is well-justified,
21

22 ⁷ Hanna Decl. Ex. F [FBI, *Going Dark*].

23 ⁸ See, e.g., Hanna Decl. Ex. L [James Comey, *Going Dark: Encryption, Technology,*
24 *and the Balances Between Public Safety and Encryption*, Joint Statement with
25 Deputy Atty. Gen. Sally Quillian Yates Before the Sen. Judiciary Comm. (July 8,
2015)]. The repeated concern about the broader “going dark” problem, and the
focus on universal back doors, stands in stark contrast to the comments by
government officials that this case is just about one iPhone.

26 ⁹ See Hanna Decl. Ex. M [Susan Landau, *The National-Security Needs for*
27 *Ubiquitous Encryption* (Feb. 1, 2016)].

28 ¹⁰ See Hanna Decl. Ex. N, ¶ 20 [Apple Inc. and Apple Distrib. Int’l, Written Evidence
(IPB0093), (Dec. 21, 2015)].

1 because “the greater public good is a secure communications infrastructure protected
2 by ubiquitous encryption at the device, server and enterprise level without building in
3 means for government monitoring.”¹¹

4 In recent years, however, the government, led by the Department of Justice, has
5 considered legislative proposals that would have mandated such a back door. Those
6 proposals sought to significantly expand the reach of the Communications Assistance
7 for Law Enforcement Act (“CALEA”), 47 U.S.C. § 1001 *et seq.*, in which Congress
8 defined the circumstances under which private companies must assist law enforcement
9 in executing authorized electronic surveillance and the nature of—and limits on—the
10 assistance such companies must provide.¹² In addressing the twin needs of law
11 enforcement and privacy, Congress, through CALEA, specified when a company has
12 an obligation to assist the government with decryption of communications, and made
13 clear that a company has no obligation to do so where, as here, the company does not
14 retain a copy of the decryption key. 47 U.S.C. § 1002(b)(3). Congress, keenly aware
15 of and focusing on the specific area of dispute here, thus opted *not* to provide authority
16 to compel companies like Apple to assist law enforcement with respect to data stored
17 on a smartphone they designed and manufactured.¹³

18
19 ¹¹ Hanna Decl. Ex. O [Mike McConnell et al., *Why The Fear Over Ubiquitous Data*
Encryption Is Overblown, Wash. Post (July 28, 2015)].

20 ¹² Following a vigorous lobbying effort led by the FBI for enhanced surveillance and
21 informational-access powers in the digital age, Congress “balance[d] three key
22 policies: (1) to preserve a narrowly focused capability for law enforcement agencies
23 to carry out properly authorized intercepts; (2) to protect privacy in the face of
24 increasingly powerful and personally revealing technologies; and (3) to avoid
25 impeding the development of new communications services and technologies.”
26 H.R. Rep. No. 103-827(I), at 13 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489,
27 3493; *see also id.* at 17, 1994 U.S.C.C.A.N. at 3497 (“[A]s the potential
28 intrusiveness of technology increases, it is necessary to ensure that government
surveillance authority is clearly defined and appropriately limited.”).

¹³ The government has acknowledged this. Dkt. 1 at 23. CALEA requires only
“telecommunications carriers” to ensure that their “equipment, facilities, or
services” enable the government to intercept communications pursuant to a court
order or other lawful authorization. 47 U.S.C. § 1002. CALEA defines
“telecommunications carrier” to exclude persons or entities providing “information
services,” such as Apple. *Id.* § 1001(8).

1 The government’s proposed changes to CALEA would have dramatically
2 expanded the law’s scope by mandating that companies install back doors into their
3 products to ensure that authorities can access encrypted data when authorized to do
4 so.¹⁴ In the face of this proposal—commonly referred to as “CALEA II”—leading
5 technology companies, including Apple, as well as public interest organizations like
6 the ACLU and Human Rights Watch, urged President Obama to “reject any proposal
7 that U.S. companies deliberately weaken the security of their products . . . [and]
8 instead focus on developing policies that will promote rather than undermine the wide
9 adoption of strong encryption technology.”¹⁵

10 The Executive Branch ultimately decided not to pursue CALEA II, and
11 Congress has left CALEA untouched, meaning that Congress never granted the
12 authority the government now asserts. Moreover, members of Congress have recently
13 introduced three pieces of legislation that would affirmatively prohibit the government
14 from forcing private companies like Apple to compromise data security.¹⁶ On October
15 8, 2015, FBI Director Comey confirmed that the Obama Administration would not
16 seek passage of CALEA II at that time.¹⁷ Instead, Director Comey expressed his view

17 ¹⁴ See Hanna Decl. Ex. P [Ellen Nakashima, *Proposal Seeks to Fine Tech Companies*
18 *for Noncompliance with Wiretap Orders*, Wash. Post (Apr. 28, 2013)].

19 ¹⁵ Hanna Decl. Ex. Q [New America’s Open Technology Institute, *Joint Letter to*
20 *President Barack Obama* (May 19, 2015)].

21 ¹⁶ See Secure Data Act of 2015, S.135, 114th Cong. (2015) (proposal to prohibit a
22 federal agency from requiring hardware or software manufacturers to design or alter
23 the security functions in their products to allow surveillance, and exempting
24 products used pursuant to CALEA); Secure Data Act of 2015, H.R. 726, 114th
25 Cong. (2015) (same); End Warrantless Surveillance of Americans Act, H.R. 2233,
26 114th Cong. (2015) (same, adding additional amendments to the Foreign
27 Intelligence Surveillance Act of 1978). In fact, just last week, four senior members
28 of the House Judiciary Committee issued a statement expressing concern that the
order in this case constitutes an “end-run around the legislative process.” Hanna
Decl. Ex. R [*Senior House Judiciary Committee Democrats Express Concern Over*
Government Attempts to Undermine Encryption, House Comm. on the Judiciary,
Democrats (Feb. 18, 2016)]. Recognizing that Congress has not yet determined to
act on this issue, they stated that “there is little reason for the government to make
this demand on Apple—except to enact a policy proposal that has gained no
traction in Congress and was rejected by the White House.” *Id.*

¹⁷ Hanna Decl. Ex. S [James Comey, *Statement Before the Senate Comm. on*
Homeland Sec. & Governmental Affairs (Oct. 8, 2015)] (noting that while the

(Cont'd on next page)

1 that the “going dark” debate raises issues that “to a democracy should be very, very
2 concerning” and therefore the issue is “worthy of a larger public conversation.”¹⁸
3 President Obama has also remarked that it is “useful to have civil libertarians and
4 others tapping us on the shoulder in the midst of this process and reminding us that
5 there are values at stake as well,” noting further that he “welcome[s] that kind of
6 debate.”¹⁹ As the President has recognized, these issues are part of “a public
7 conversation that we should end up having.”²⁰

8 **C. Apple’s Substantial Assistance In The Government’s Investigation**

9 Apple was shocked and saddened by the mindless savagery of the December 2,
10 2015 terrorist attack in San Bernardino. In the days following the attack, the FBI
11 approached Apple for help in its investigation. Apple responded immediately, and
12 devoted substantial resources on a 24/7 basis to support the government’s investigation
13 of this heinous crime. Declaration of Lisa Olle (“Olle Decl.”) ¶¶ 5-9.

14 Apple promptly provided all data that it possessed relating to the attackers’
15 accounts and that the FBI formally requested via multiple forms of legal process, in
16 keeping with Apple’s commitment to comply with all legally valid subpoenas and

17
18

(Cont'd from previous page)

19 “United States government is actively engaged with private companies to ensure
20 they understand the public safety and national security risks that result from
malicious actors’ use of their encrypted products and services . . . the administration
is not seeking legislation at this time.”).

21 ¹⁸ See Hanna Decl. Ex. T [James Comey, *Director Discusses Encryption, Patriot Act*
22 *Provisions*, (May 20, 2015)]. Even Manhattan District Attorney Cyrus Vance, Jr.,
23 who is eager to see the government prevail here, has acknowledged that these issues
24 should be resolved by Congress. Hanna Decl. Ex. Z [Cyrus R. Vance Jr., *No*
Smartphone Lies Beyond the Reach of a Judicial Search Warrant, N.Y. Times (Feb.
25 18, 2016)]; Hanna Decl. Ex. U [NPR, Weekend Edition, *It’s Not Just the iPhone*
Law Enforcement Wants to Unlock (Feb. 21, 2016)] (“ . . . I think that the United
26 States Congress is going to have to step in here . . . We need to look at this with
27 independent eyes. And I believe Congress ultimately is going to have to make the
28 judgment call of where we draw that line [between privacy and public safety]”).

¹⁹ Hanna Decl. Ex. V [*Remarks by President Obama and Prime Minister Cameron of*
the United Kingdom in Joint Press Conference (Jan. 16, 2015)].

²⁰ Hanna Decl. Ex. W [Kara Swisher, *White House. Red Chair. Obama Meets*
Swisher, Re/Code.com (Feb. 15, 2015)].

1 search warrants that the company receives. *Id.* Additionally, Apple has furnished
2 valuable informal assistance to the government’s investigation—participating in
3 teleconferences, providing technical assistance, answering questions from the FBI, and
4 suggesting potential alternatives for the government to attempt to obtain data from the
5 iPhone at issue. *Id.* ¶ 6.

6 Unfortunately, the FBI, without consulting Apple or reviewing its public
7 guidance regarding iOS, changed the iCloud password associated with one of the
8 attacker’s accounts, foreclosing the possibility of the phone initiating an automatic
9 iCloud back-up of its data to a known Wi-Fi network, *see* Hanna Decl. Ex. X [Apple
10 Inc., *iCloud: Back up your iOS device to iCloud*], which could have obviated the need
11 to unlock the phone and thus for the extraordinary order the government now seeks.²¹
12 Had the FBI consulted Apple first, this litigation may not have been necessary.

13 **D. The Government’s *Ex Parte* Application Under The All Writs Act, And**
14 **This Court’s Order**

15 On February 16, 2016, the government filed an *ex parte* application and
16 proposed order asking the Court to compel Apple to assist in the government’s
17 investigation under the authority of the All Writs Act, codified at 28 U.S.C. § 1651.²²

18 ²¹ In its motion to compel, filed February 19 with this Court, the government sought
19 to shift the blame to the “owner” (San Bernardino County) in describing who
20 changed the password and why it allegedly has no other viable alternatives besides
21 the creation of a new operating system. Dkt. 1 at 18 n.7. The FBI later issued a
22 press release acknowledging that it “worked with” the County to reset the
password. *See* Hanna Decl. Ex. Y [*Statement to Address Misleading Reports that*
the County of San Bernardino Reset Terror Suspect’s iPhone Without Consent of
the FBI, issued by the FBI to Ars Technica (Feb. 21, 2016)].

23 ²² The government obtained the Order without notice to Apple and without allowing
24 Apple an opportunity to be heard. *See Mullane v. Cent. Hanover Bank & Tr. Co.*,
25 339 U.S. 306, 314 (1950) (recognizing that one of the “fundamental requisite[s] of
26 due process of law is the opportunity to be heard”) (quoting *Grannis v. Ordean*,
27 234 U.S. 385, 394 (1914)). But this was not a case where the government needed
28 to proceed in secret to safeguard its investigation; indeed, Apple understands that
the government alerted reporters before filing its *ex parte* application, and then,
immediately after it was signed and confirmed to be on the docket, distributed the
application and Order to the public at about the same time it notified Apple.
Moreover, this is the only case in counsel’s memory in which an FBI Director has
blogged in real-time about pending litigation, suggesting that the government does
not believe the data on the phone will yield critical evidence about other suspects.

(*Cont’d on next page*)

1 With no opposition or other perspectives to consider, the Court granted the
2 government’s request and signed the government’s proposed order, thereby compelling
3 Apple to create new software that would allow the government to hack into an iPhone
4 5c used by one of the attackers. Order Compelling Apple Inc. to Assist Agents in
5 Search, *In the Matter of the Search of an Apple iPhone Seized During the Execution of*
6 *a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203*, No. ED 15-
7 0451M (Feb. 16, 2016), Dkt. at 19 (the “Order”).

8 The Order directs Apple to provide “reasonable technical assistance to assist law
9 enforcement agents in obtaining access to the data” on the device. *Id.* ¶ 1. The Order
10 further defines this “reasonable technical assistance” to include creating custom
11 software that can be loaded on the iPhone to accomplish three goals: (1) bypass or
12 disable the iPhone’s “auto-erase” function, designed to protect against efforts to obtain
13 unauthorized access to the device’s encrypted contents by deleting encrypted data after
14 ten unsuccessful attempts to enter the iPhone’s passcode, (2) enable the FBI to
15 electronically submit passcodes to the device for testing, bypassing the requirement
16 that passcodes be manually entered, and (3) remove any time delays between entering
17 incorrect passcodes. *Id.* ¶ 2. Because the government proceeded *ex parte*, Apple had
18 no opportunity to weigh in on whether such assistance was “reasonable,” and thus the
19 government’s request was assumed to be.

20 The software envisioned by the government simply does not exist today. Thus,
21 at bottom, the Order would compel Apple to create a new version of the iPhone
22 operating system designed to defeat the critical security features noted previously for
23 the specific purpose of accessing the device’s contents in unencrypted form—in other
24 words, to write new software to create a back door to the device’s encrypted data.

25
26 _____
27 (*Cont'd from previous page*)

28 See Hanna Decl. Ex. G [Comey, *Going Dark*]; Hanna Decl. Ex. H [Comey, *Follow This Lead*].

1 **E. The Resources And Effort Required To Develop The Software Demanded**
2 **By The Government**

3 The compromised operating system that the government demands would require
4 significant resources and effort to develop. Although it is difficult to estimate, because
5 it has never been done before, the design, creation, validation, and deployment of the
6 software likely would necessitate six to ten Apple engineers and employees dedicating
7 a very substantial portion of their time for a minimum of two weeks, and likely as
8 many as four weeks. Neuenschwander Decl. ¶ 22. Members of the team would
9 include engineers from Apple’s core operating system group, a quality assurance
10 engineer, a project manager, and either a document writer or a tool writer. *Id.*

11 No operating system currently exists that can accomplish what the government
12 wants, and any effort to create one will require that Apple write new code, not just
13 disable existing code functionality. *Id.* ¶ 24–25. Rather, Apple will need to design and
14 implement untested functionality in order to allow the capability to enter passcodes
15 into the device electronically in the manner that the government describes. *Id.* ¶ 24. In
16 addition, Apple would need to either develop and prepare detailed documentation for
17 the above protocol to enable the FBI to build a brute-force tool that is able to interface
18 with the device to input passcode attempts, or design, develop and prepare
19 documentation for such a tool itself. *Id.* ¶ 25. Further, if the tool is utilized remotely
20 (rather than at a secure Apple facility), Apple will also have to develop procedures to
21 encrypt, validate, and input into the device communications from the FBI. *Id.* This
22 entire development process would need to be logged and recorded in case Apple’s
23 methodology is ever questioned, for example in court by a defense lawyer for anyone
24 charged in relation to the crime. *Id.* ¶ 28.

25 Once created, the operating system would need to go through Apple’s quality
26 assurance and security testing process. *Id.* ¶ 29. Apple’s software ecosystem is
27 incredibly complicated, and changing one feature of an operating system often has
28 ancillary or unanticipated consequences. *Id.* ¶ 30. Thus, quality assurance and
security testing would require that the new operating system be tested on multiple

1 devices and validated before being deployed. *Id.* Apple would have to undertake
2 additional testing efforts to confirm and validate that running this newly developed
3 operating system to bypass the device’s security features will not inadvertently destroy
4 or alter any user data. *Id.* ¶ 31. To the extent problems are identified (which is almost
5 always the case), solutions would need to be developed and re-coded, and testing
6 would begin anew. *Id.* ¶ 32. As with the development process, the entire quality
7 assurance and security testing process would need to be logged, recorded, and
8 preserved. *Id.* ¶ 33. Once the new custom operating system is created and validated, it
9 would need to be deployed on to the subject device, which would need to be done at an
10 Apple facility. *Id.* ¶¶ 34-35. And if the new operating system has to be destroyed and
11 recreated each time a new order is issued, the burden will multiply. *Id.* ¶¶ 44-45.

12 III. ARGUMENT

13 A. **The All Writs Act Does Not Provide A Basis To Conscript Apple To Create 14 Software Enabling The Government To Hack Into iPhones.**

15 The All Writs Act (or the “Act”) does not provide the judiciary with the
16 boundless and unbridled power the government asks this Court to exercise. The Act is
17 intended to enable the federal courts to fill in gaps in the law so they can exercise the
18 authority they already possess by virtue of the express powers granted to them by the
19 Constitution and Congress; it does not grant the courts free-wheeling authority to
20 change the substantive law, resolve policy disputes, or exercise new powers that
21 Congress has not afforded them. Accordingly, the Ninth Circuit has squarely rejected
22 the notion that “the district court has such wide-ranging inherent powers that it can
23 impose a duty on a private party *when Congress has failed to impose one*. To so rule
24 would be to usurp the legislative function and to improperly extend the limited federal
25 court jurisdiction.” *Plum Creek*, 608 F.2d at 1290 (emphasis added).

26 Congress has never authorized judges to compel innocent third parties to
27 provide decryption services to the FBI. Indeed, Congress has expressly withheld that
28 authority in other contexts, and this issue is currently the subject of a raging national

1 policy debate among members of Congress, the President, the FBI Director, and state
2 and local prosecutors. Moreover, federal courts themselves have *never* recognized an
3 inherent authority to order non-parties to become de facto government agents in
4 ongoing criminal investigations. Because the Order is not grounded in any duly
5 enacted rule or statute, and goes well beyond the very limited powers afforded by
6 Article III of the Constitution and the All Writs Act, it must be vacated.

7 **1. The All Writs Act Does Not Grant Authority To Compel Assistance**
8 **Where Congress Has Considered But Chosen Not To Confer Such**
9 **Authority.**

10 The authority the government seeks here cannot be justified under the All Writs
11 Act because law enforcement assistance by technology providers is covered by
12 existing laws that specifically omit providers like Apple from their scope. The All
13 Writs Act authorizes courts to “issue all writs necessary or appropriate in aid of their
14 respective jurisdictions and agreeable to the usages and principles of law,” 28 U.S.C.
15 § 1651(a), but as the Supreme Court has held, it “does not authorize [courts] to issue
16 ad hoc writs whenever compliance with statutory procedures appears inconvenient or
17 less appropriate,” *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 38, 43
18 (1985) (holding that the Act did not confer power on the district court to compel non-
19 custodians to bear the expense of producing the prisoner-witnesses); *see also In the*
20 *Matter of an Application of U.S. of Am. for an Order Authorizing Disclosure of*
21 *Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 578 (D. Md. 2011)
22 (holding that the Act does not authorize an “end run around constitutional and statutory
23 law”). The Ninth Circuit likewise has emphasized that the “All Writs Act is not a
24 grant of plenary power to federal courts. Rather, it is designed to aid the courts in the
25 exercise of their jurisdiction.” *Plum Creek*, 608 F.2d at 1289 (holding that the Act
26 “does not give the district court a roving commission to order a party subject to an
27 investigation to accept additional risks at the bidding” of the government); *see also Ex*
28 *parte Bollman*, 8 U.S. 75 (1807) (“[C]ourts which are created by written law, and
whose jurisdiction is defined by written law, cannot transcend that jurisdiction.”).

1 Thus, in another pending case in which the government seeks to compel Apple to assist
2 in obtaining information from a drug dealer’s iPhone, Magistrate Judge Orenstein
3 issued an order stating that while the Act may be appropriately invoked “to fill in a
4 statutory gap that Congress has failed to consider,” it cannot be used to grant the
5 government authority “Congress chose not to confer.” *In re Order Requiring Apple,*
6 *Inc. to Assist in the Execution of a Search Warrant Issued by this Court (“In re*
7 *Order”),* No. 15-MC-1902, 2015 WL 5920207, at *2 (E.D.N.Y. Oct. 9, 2015).

8 Congress knows how to impose a duty on third parties to facilitate the
9 government’s decryption of devices. Similarly, it knows exactly how to place limits
10 on what the government can require of telecommunications carriers and also on
11 manufacturers of telephone equipment and handsets. And in CALEA, Congress
12 decided not to require electronic communication service providers, like Apple, to do
13 what the government seeks here. Contrary to the government’s contention that
14 CALEA is inapplicable to this dispute, Congress declared via CALEA that the
15 government cannot dictate to providers of electronic communications services or
16 manufacturers of telecommunications equipment any specific equipment design or
17 software configuration.

18 In the section of CALEA entitled “Design of features and systems
19 configurations,” 47 U.S.C. § 1002(b)(1), the statute says that it “does not authorize any
20 law enforcement agency or officer—

- 21 (1) to require any specific design of equipment, facilities, services,
22 features, or system configurations to be adopted by any provider of
23 a wire or electronic communication service, any manufacturer of
24 telecommunications equipment, or any provider of
25 telecommunications support services.
- 26 (2) to prohibit the adoption of any equipment, facility, service, or
27 feature by any provider of a wire or electronic communication
28 service, any manufacturer of telecommunications equipment, or any
provider of telecommunications support services.

Apple unquestionably serves as a provider of “electronic communications services”
through the various messaging services it provides to its customers through iPhones.

1 *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 901 (9th Cir. 2008).
2 Apple also makes mobile phones. As such, CALEA does not allow a law enforcement
3 agency to require Apple to implement any specific design of its equipment, facilities,
4 services or system configuration. Yet, that is precisely what the government seeks
5 here. Thus, CALEA’s restrictions are directly on point.

6 Moreover, CALEA also intentionally excludes “information services providers,”
7 like Apple, from the scope of its mandatory assistance provisions.²³ This exclusion
8 precludes the government from using the All Writs Act to require Apple to do that
9 which Congress eschewed. But even if Apple were covered by CALEA, the law does
10 not require covered telecommunication carriers (which Apple is not) to be responsible
11 for “decrypting, or *ensuring the government’s ability to decrypt*, any communication
12 encrypted by a subscriber or customer unless the encryption was provided by the
13 carrier and the carrier possesses the information necessary to decrypt the
14 communication.” 47 U.S.C. § 1002(b)(3) (emphasis added).

15 Thus, here again, CALEA makes a specific choice to allow strong encryption (or
16 any other security feature or configuration) with keys chosen by end users to be
17 deployed, and prevents the government from mandating that such encryption schemes
18 contain a “back door.” *See also* H.R. Rep. 103-827(I), at 24, 1994 U.S.C.C.A.N. 3489,
19 3504 (emphasizing that CALEA does not “prohibit a carrier from deploying an
20 encryption service for which it does not retain the ability to decrypt communications
21 for law enforcement access”; “[n]or does the Committee intend this bill to be in any
22 way a precursor to any kind of ban or limitation on encryption technology. To the
23 contrary, [§ 1002] protects the right to use encryption.”).

24 Similarly, outside of CALEA, Congress also knows how to require third parties
25 to provide “technical assistance,” *see* Wiretap Act, 18 U.S.C. § 2518(4) (providing that

26 ²³ Information service providers are defined to include services that permit a customer
27 to retrieve stored information from, or file information for storage in, information
28 storage facilities; electronic publishing; and electronic messaging services. *See* 47
U.S.C. § 1001.

1 upon the lawful execution of a wiretap, the government can seek an order compelling a
2 third party to furnish “all information, facilities, and technical assistance necessary to
3 accomplish the interception”); Pen/Trap Statute, *id.* § 3123(b)(2) (similar), but
4 Congress has intentionally opted not to compel third parties’ assistance in retrieving
5 stored information on devices. That Congress, confronted over the years with the
6 contentious debate about where to draw the lines among competing security and
7 privacy interests, made this decision, “indicates a deliberate congressional choice with
8 which the courts should not interfere.” *Cent. Bank of Denver, N.A. v. First Interstate*
9 *Bank of Denver, N.A.*, 511 U.S. 164, 184 (1994). The Executive Branch, having
10 considered and then declined to urge Congress to amend CALEA to enable it to
11 compel the type of assistance demanded here, cannot seek that same authority via an *ex*
12 *parte* application for a court order under the Act.

13 For the courts to use the All Writs Act to expand sub rosa the obligations
14 imposed by CALEA as proposed by the government here would not just exceed the
15 scope of the statute, but it would also violate the separation-of-powers doctrine. Just
16 as the “Congress may not exercise the judicial power to revise final judgments,”
17 *Clinton v. Jones*, 520 U.S. 681, 699 (1997) (citing *Plaut v. Spendthrift Farm, Inc.*, 514
18 U.S. 211 (1995)), courts may not exercise the legislative power by repurposing statutes
19 to meet the evolving needs of society, *see Clark v. Martinez*, 543 U.S. 371, 391 (2005)
20 (court should “avoid inventing a statute rather than interpreting one”) (citation,
21 quotation marks, and alterations omitted); *see also Alzheimer’s Inst. of Am. Inc. v. Elan*
22 *Corp.*, 2013 WL 8744216, at *2 (N.D. Cal. Jan. 31, 2013) (Congress alone has
23 authority “to update” a “technologically antiquated” statute “to address the new and
24 rapidly evolving era of computer and cloud-stored, processed and produced
25 data”). Nor does Congress lose “its exclusive constitutional authority to make laws
26 necessary and proper to carry out the powers vested by the Constitution” in times of
27 crisis (whether real or imagined). *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S.
28 579, 588–89 (1952). Because a “decision to rearrange or rewrite [a] statute falls within

1 the legislative, not the judicial prerogative[,]” the All Writs Act cannot possibly be
2 deemed to grant to the courts the extraordinary power the government seeks. *Xi v.*
3 *INS*, 298 F.3d 832, 839 (9th Cir. 2002).

4 If anything, whether companies like Apple should be compelled to create a back
5 door to their own operating systems to assist law enforcement is a political question,
6 not a legal one. See *Baker v. Carr*, 369 U.S. 186, 217 (1962) (holding that a case is a
7 nonjusticiable political question if it is impossible to decide “without an initial policy
8 determination of a kind clearly for nonjudicial discretion”); see also *Vieth v. Jubelirer*,
9 541 U.S. 267, 277–290 (2004) (plurality opinion) (dismissing claims of political
10 gerrymandering under the political question doctrine because there was no “judicially
11 discoverable and manageable standard for resolving” them); *Diamond v. Chakrabarty*,
12 447 U.S. 303, 317 (1980) (“The choice [the court is] urged to make is a matter of high
13 policy for resolution within the legislative process after the kind of investigation,
14 examination, and study that legislative bodies can provide and courts cannot.”);
15 *Saldana v. Occidental Petroleum Corp.*, 774 F.3d 544, 552 (9th Cir. 2014) (per
16 curiam) (affirming district court’s holding that the claims were “inextricably bound to
17 an inherently political question” and thus were “beyond the jurisdiction of our courts”).

18 In short, a decision to “short-circuit public debate on this controversy seems
19 fundamentally inconsistent with the proposition that such important policy issues
20 should be determined in the first instance by the legislative branch after public
21 debate—as opposed to having them decided by the judiciary in sealed, *ex parte*
22 proceedings.” *In re Order*, 2015 WL 5920207, at *3 n.1. Such an important decision
23 with such widespread global repercussions goes well beyond the purview of the All
24 Writs Act, which merely provides courts with a limited grant of ancillary authority to
25 issue orders “in aid of their respective jurisdictions.” 28 U.S.C. § 1651(a).

1 **2. *New York Telephone Co. And Its Progeny Confirm That The All***
2 ***Writs Act Does Not Authorize Courts To Compel The Unprecedented***
3 ***And Unreasonably Burdensome Conscription Of Apple That The***
4 ***Government Seeks.***

5 The government relies heavily on the Supreme Court’s decision in *United States*
6 *v. New York Telephone Co.*, 434 U.S. 159 (1977), to assert that the All Writs Act
7 permits the Court to compel private third parties like Apple to assist the government in
8 effectuating a search warrant by writing new software code that would undermine the
9 security of its own product. The government misapplies this case.

10 In *New York Telephone Co.*, the district court compelled the company to install a
11 simple pen register device (designed to record dialed numbers) on two telephones
12 where there was “probable cause to believe that the [c]ompany’s facilities were being
13 employed to facilitate a criminal enterprise on a continuing basis.” 434 U.S. at 174.
14 The Supreme Court held that the order was a proper writ under the Act, because it was
15 consistent with Congress’s intent to compel third parties to assist the government in the
16 use of surveillance devices, and it satisfied a three-part test imposed by the Court.

17 First, the Court found that the company was not “so far removed from the
18 underlying controversy that its assistance could not be permissibly compelled.” *Id.*
19 Second, the assistance sought was “meager,” and as a public utility, the company did
20 not “ha[ve] a substantial interest in not providing assistance.” *Id.* Third, “after an
21 exhaustive search,” the FBI was unable to find a suitable location to install its own pen
22 registers without tipping off the targets, and thus there was “no conceivable way in
23 which the surveillance authorized by the District Court could have been successfully
24 accomplished” without the company’s meager assistance. *Id.* at 175. Applying these
25 factors to this case confirms that the All Writs Act does not permit the Court to compel
26 the unprecedented and unreasonably burdensome assistance that the government seeks.

27 **a. Apple’s Connection To The Underlying Case Is “Far Removed”**
28 **And Too Attenuated To Compel Its Assistance**

 Nothing connects Apple to this case such that it can be drafted into government
 service to write software that permits the government to defeat the security features on

1 Apple's standard operating system. Apple is a private company that does not own or
2 possess the phone at issue, has no connection to the data that may or may not exist on
3 the phone, and is not related in any way to the events giving rise to the investigation.
4 This case is nothing like *New York Telephone Co.*, where there was probable cause to
5 believe that the phone company's own facilities were "being employed to facilitate a
6 criminal enterprise on a continuing basis." *Id.* at 174.

7 The government relies on *United States v. Hall*, 583 F. Supp. 717 (E.D. Va.
8 1984), and *In re Application of U.S. of Am. for an Order Directing X to Provide Access*
9 *to Videotapes* ("Videotapes"), 2003 WL 22053105 (D. Md. Aug. 22, 2003), but these
10 cases involved mere requests to produce existing business records, not the compelled
11 creation of intellectual property. In *Hall*, the court found that the All Writs Act
12 permitted an order compelling a credit card company to produce the credit card records
13 of a federal fugitive's former girlfriend, because the government had reason to believe
14 that she was harboring and supporting the fugitive, and thus potentially using her credit
15 card to perpetrate an ongoing crime. 583 F. Supp. at 720 (reasoning that a credit card
16 issuer "has an interest" in a transaction "when a credit card is used for an illegal
17 purpose even though the act itself be not illegal"). Similarly, in *Videotapes*, the court
18 compelled an apartment complex to provide access to videotape surveillance footage
19 of a hallway in the apartment to assist with executing an arrest warrant on a fugitive.
20 2003 WL 22053105, at *3. This case is nothing like *Hall* and *Videotapes*, where the
21 government sought assistance effectuating an arrest warrant to halt ongoing criminal
22 activity, since any criminal activity linked to the phone at issue here ended more than
23 two months ago when the terrorists were killed.

24 Further, unlike a telecommunications monopoly, Apple is not a "highly
25 regulated public utility with a duty to serve the public." *New York Telephone Co.*, 434
26 U.S. at 174; *see also Application of U.S. of Am. for an Order Authorizing an In-*
27 *Progress Trace of Wire Commc'ns over Tel. Facilities* ("*Mountain Bell*"), 616 F.2d
28 1122, 1132 (9th Cir. 1980) (discussing *New York Telephone Co.* and noting that its

1 ruling compelling assistance under the All Writs Act relied “[t]o a great extent . . .
2 upon the highly regulated, public nature” of the phone company); *In re Order*, 2015
3 WL 5920207, at *4–5. Whereas public utilities have no “substantial interest in not
4 providing assistance” to the government, 434 U.S. at 174, and “enjoy a monopoly in an
5 essential area of communications,” *Mountain Bell*, 616 F.2d at 1131, Apple is a private
6 company that believes that encryption is crucial to protect the security and privacy
7 interests of citizens who use and store their most personal data on their iPhones, “from
8 our private conversations to our photos, our music, our notes, our calendars and
9 contacts, our financial information and health data, even where we have been and
10 where we are going.” Hanna Decl. Ex. D at 1 [Apple Inc., *A Message to Our*
11 *Customers* (Feb. 16, 2016)].

12 That Apple “designed, manufactured and sold the SUBJECT DEVICE, and
13 wrote and owns the software that runs the phone,” Memorandum of Points and
14 Authorities in Support of Government’s *Ex Parte* Application for Order Compelling
15 Apple Inc. to Assist Agents in Search, *In the Matter of the Search of an Apple iPhone*
16 *Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal.*
17 *License Plate 35KGD203*, No. ED 15-0451M (Feb. 16, 2016), Dkt. 18 at 11 (the “*Ex*
18 *Parte App.*”), is insufficient to establish the connection mandated by *New York*
19 *Telephone Co.* The All Writs Act does not allow the government to compel a
20 manufacturer’s assistance merely because it has placed a good into the stream of
21 commerce. Apple is no more connected to this phone than General Motors is to a
22 company car used by a fraudster on his daily commute. Moreover, that Apple’s
23 software is “licensed, not sold,” *Ex Parte App.* at 5, is “a total red herring,” as Judge
24 Orenstein already concluded, Hanna Decl. Ex. DD at 42:4–10 [*In re Order Requiring*
25 *Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court*,
26 E.D.N.Y No. 15 MC 1902, Dkt. 19 (“October 26, 2015 Transcript”)]. A licensing
27 agreement no more connects Apple to the underlying events than a sale. The license
28 does not permit Apple to invade or control the private data of its customers. It merely

1 limits customers' use and redistribution of Apple's software. Indeed, the government's
2 position has no limits and, if accepted, would eviscerate the "remoteness" factor
3 entirely, as any company that offers products or services to consumers could be
4 conscripted to assist with an investigation, no matter how attenuated their connection
5 to the criminal activity. This is not, and never has been, the law.

6 **b. The Order Requested By The Government Would Impose An**
7 **Unprecedented And Oppressive Burden On Apple And Citizens**
8 **Who Use The iPhone.**

9 An order pursuant to the All Writs Act "must not [1] adversely affect the basic
10 interests of the third party or [2] impose an undue burden." *Hall*, 583 F. Supp. at 719.
11 The Order violates both requirements by conscripting Apple to develop software that
12 does not exist and that Apple has a compelling interest in not creating. The
13 government's request violates the first requirement—that the Act "must not adversely
14 affect the basic interests of the third party"—because Apple has a strong interest in
15 safeguarding its data protection systems that ensure the security of hundreds of
16 millions of customers who depend on and store their most confidential data on their
17 iPhones. An order compelling Apple to create software that defeats those safeguards
18 undeniably threatens those systems and adversely affects Apple's interests and those of
19 iPhone users around the globe. *See id.*

20 The government's request violates the second requirement—that the Act "must
21 not . . . impose an undue burden"—because the government's unprecedented demand
22 forces Apple to develop new software that destroys the security features that Apple has
23 spent years building. As discussed *supra* in section II.E, no operating system currently
24 exists that can accomplish what the government wants, and any effort to create one
25 would require that Apple write new code, not just disable existing functionality.
26 Neuenschwander Decl. ¶¶ 23-25. Experienced Apple engineers would have to design,
27 create, test, and validate the compromised operating system, using a hyper-secure
28 isolation room within which to do it, and then deploy and supervise its operation by the
FBI to brute force crack the phone's passcode. *Id.* ¶¶ 21-43; Olle Decl. ¶ 14. The

1 system itself would have to be tested on multiple devices to ensure that the operating
2 system works and does not alter any data on the device. Neuenschwander ¶¶ 30-31.
3 All aspects of the development and testing processes would need to be logged and
4 recorded in case Apple’s methodology is ever questioned. *Id.* ¶¶ 28, 33.

5 Moreover, the government’s flawed suggestion to delete the program and erase
6 every trace of the activity would not lessen the burden, it would actually increase it
7 since there are hundreds of demands to create and utilize the software waiting in the
8 wings. *Id.* ¶¶ 38-45. If Apple creates new software to open a back door, other federal
9 and state prosecutors—and other governments and agencies—will repeatedly seek
10 orders compelling Apple to use the software to open the back door for tens of
11 thousands of iPhones. Indeed, Manhattan District Attorney Cyrus Vance, Jr., has made
12 clear that the federal and state governments want access to *every* phone in a criminal
13 investigation.²⁴ See Hanna Decl., Ex. Z [(Cyrus R. Vance, Jr., *No Smartphone Lies*
14 *Beyond the Reach of a Judicial Search Warrant*, N.Y. Times (Feb. 18, 2016)]; Hanna
15 Decl. ¶ 5 at 18:28 [Charlie Rose, Television Interview of Cyrus Vance (Feb. 18, 2016)]
16 (Vance stating “absolutely” that he “want[s] access to all those phones that [he thinks]
17 are crucial in a criminal proceeding”). This enormously intrusive burden—building
18 everything up and tearing it down for each demand by law enforcement—lacks any
19 support in the cases relied on by the government, nor do such cases exist.

21 ²⁴ Use of the software in criminal prosecutions only exacerbates the risk of disclosure,
22 given that criminal defendants will likely challenge its reliability. See Fed. R. Evid.
23 702 (listing requirements of expert testimony, including that “testimony [be] the
24 product of reliable principles and methods” and “the expert has reliably applied the
25 principles and methods to the facts of the case,” all of which a defendant is entitled
26 to challenge); see also *United States v. Budziak*, 697 F.3d 1105, 1111–13 (9th Cir.
27 2012) (vacating order denying discovery of FBI software); *State v. Underdahl*, 767
28 N.W.2d 677, 684–86 (Minn. 2009) (upholding order compelling discovery of
breathalyzer source code). The government’s suggestion that Apple can destroy the
software has clearly not been thought through, given that it would jeopardize
criminal cases. See *United States v. Cooper*, 983 F.2d 928, 931–32 (9th Cir. 1993)
(government’s bad-faith failure to preserve laboratory equipment seized from
defendants violated due process, and appropriate remedy was dismissal of
indictment, rather than suppression of evidence).

1 The alternative—keeping and maintaining the compromised operating system
2 and everything related to it—imposes a different but no less significant burden, *i.e.*,
3 forcing Apple to take on the task of unfailingly securing against disclosure or
4 misappropriation the development and testing environments, equipment, codebase,
5 documentation, and any other materials relating to the compromised operating system.
6 *Id.* ¶ 47. Given the millions of iPhones in use and the value of the data on them,
7 criminals, terrorists, and hackers will no doubt view the code as a major prize and can
8 be expected to go to considerable lengths to steal it, risking the security, safety, and
9 privacy of customers whose lives are chronicled on their phones. Indeed, as the
10 Supreme Court has recognized, “[t]he term ‘cell phone’ is itself misleading shorthand;
11 . . . these devices are in fact minicomputers” that “could just as easily be called
12 cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums,
13 televisions, maps, or newspapers.” *Riley v. California*, 134 S. Ct. 2473, 2488–89
14 (2014) (observing that equating the “data stored on a cell phone” to “physical items”
15 “is like saying a ride on horseback is materially indistinguishable from a flight to the
16 moon”). By forcing Apple to write code to compromise its encryption defenses, the
17 Order would impose substantial burdens not just on Apple, but on the public at large.
18 And in the meantime, nimble and technologically savvy criminals will continue to use
19 other encryption technologies, while the law-abiding public endures these threats to
20 their security and personal liberties—an especially perverse form of unilateral
21 disarmament in the war on terror and crime. *See n.4 supra* (describing ISIS’s shift to
22 more secure communication methods).

23 In addition, compelling Apple to create software in this case will set a dangerous
24 precedent for conscripting Apple and other technology companies to develop
25 technology to do the government’s bidding in untold future criminal investigations. If
26 the government can invoke the All Writs Act to compel Apple to create a special
27 operating system that undermines important security measures on the iPhone, it could
28 argue in future cases that the courts should compel Apple to create a version to track

1 the location of suspects, or secretly use the iPhone’s microphone and camera to record
2 sound and video. And if it succeeds here against Apple, there is no reason why the
3 government could not deploy its new authority to compel other innocent and unrelated
4 third-parties to do its bidding in the name of law enforcement. For example, under the
5 same legal theories advocated by the government here, the government could argue
6 that it should be permitted to force citizens to do all manner of things “necessary” to
7 assist it in enforcing the laws, like compelling a pharmaceutical company against its
8 will to produce drugs needed to carry out a lethal injection in furtherance of a lawfully
9 issued death warrant,²⁵ or requiring a journalist to plant a false story in order to help
10 lure out a fugitive, or forcing a software company to insert malicious code in its auto-
11 update process that makes it easier for the government to conduct court-ordered
12 surveillance. Indeed, under the government’s formulation, any party whose assistance
13 is deemed “necessary” by the government falls within the ambit of the All Writs Act
14 and can be compelled to do anything the government needs to effectuate a lawful court
15 order. While these sweeping powers might be nice to have from the government’s
16 perspective, they simply are not authorized by law and would violate the Constitution.

17 Moreover, responding to these demands would effectively require Apple to
18 create full-time positions in a new “hacking” department to service government
19 requests and to develop new versions of the back door software every time iOS
20 changes, and it would require Apple engineers to testify about this back door as
21 government witnesses at trial. *See, e.g., United States v. Cameron*, 699 F.3d 621, 643–
22 44 (1st Cir. 2012) (holding that reports generated by an Internet provider were
23 testimonial, and thus could not be admitted without “giving [defendant] the
24 opportunity to cross-examine the [provider’s] employees who prepared the []
25 [r]eports”). Nothing in federal law allows the courts, at the request of prosecutors, to

26
27 ²⁵ Magistrate Judge Orenstein posed this same hypothetical to the government, and
28 the government had no answer. Hanna Decl. Ex. DD at 43–47 [October 26, 2015
Transcript].

1 coercively deputize Apple and other companies to serve as a permanent arm of the
2 government’s forensics lab. Indeed, the government fails to cite any case—because
3 none exists—to support its incorrect contention that courts have invoked the All Writs
4 Act to conscript a company like Apple to “to write some amount of code in order to
5 gather information in response to subpoenas or other process.” Ex Parte App. at 15.

6 The burden imposed on Apple is thus in sharp contrast to *New York Telephone*
7 *Co.*, where the public utility was compelled to provide “meager assistance” in setting
8 up a pen register—a step which “required minimal effort on the part of the [c]ompany
9 and no disruption to its operations.” 434 U.S. at 174–75 (noting that the company
10 routinely employed pen registers without court order for purposes of checking billing
11 operations and detecting fraud); *see also Mountain Bell*, 616 F.2d at 1132 (order
12 compelling the phone company to use a tracing technique akin to a pen register did not
13 impose a substantial burden because it “was extremely narrow in scope,” and
14 “prohibit[ed] any tracing technique which required active monitoring by company
15 personnel”). The very limited orders in those cases thus “should not be read to
16 authorize the wholesale imposition upon private, third parties of duties pursuant to
17 search warrants.” *Id.*

18 The other cases the government relies on involve similarly inconsequential
19 burdens where third parties were asked to turn over records that were already in their
20 possession or readily accessible, *Videotapes*, 2003 WL 22053105, at *3 (directing
21 apartment complex owner to share surveillance footage “maintained in the ordinary
22 course of business”); *Hall*, 583 F. Supp. at 722 (directing bank to produce credit card
23 records), or where the third party provided minimal assistance to effect a lawful
24 wiretap, *In re Application of U.S. of Am. for an Order Directing a Provider of*
25 *Comm’n Servs. to Provide Tech. Assistance to Agents of the U.S. Drug Enf’t Admin.*,
26 2015 WL 5233551, at *5 (D.P.R. Aug. 27, 2015). But unlike those cases, where the
27 government directed a third party to provide something that already existed or sought
28 assistance with a minimal and routine service, here the government wants to compel

1 Apple to deploy a team of engineers to write and test software code and create a new
2 operating system that undermines the security measures it has worked so hard to
3 establish—and then to potentially do that over and over again as other federal, state,
4 local and foreign prosecutors make demands for the same thing.

5 The government’s reliance on two phone “unlocking” cases is similarly
6 misplaced. Ex Parte App. at 9 (citing *United States v. Navarro*, No. 13-CR-5525
7 (W.D. Wash. Nov. 13, 2013), ECF No. 39; *In re Order Requiring [XXX], Inc. to Assist*
8 *in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone*,
9 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014) (“*Order Requiring [XXX]*”). As an
10 initial matter, the *Navarro* order is a minute order that does not contain any analysis of
11 the All Writs Act, and it is unclear whether its limitations were ever raised or
12 considered. The *Navarro* order is also distinguishable because it involved the
13 government’s request to unlock an iPhone on an older operating system that did *not*
14 require the creation of any new software. *Order Requiring [XXX]*, which was also
15 issued without the benefit of adversarial briefing, is equally unavailing. 2014 WL
16 5510865, at *3 (granting *ex parte* application to compel a third party to bypass a lock
17 screen on a phone to effectuate a search warrant). Although the court purported to
18 apply *New York Telephone Co.*, it did not analyze all of the factors set forth in that
19 case, such as whether the All Writs Act could be used to compel third parties to hack
20 into phones, whether the cellphone company was “too far removed” from the matter,
21 or whether hacking into the phone adversely affected the company’s interests. Rather,
22 the court simply concluded the technical service sought was not “burdensome,” akin to
23 “punching a few buttons” or installing a pen register. 2014 WL 5510865, at *2
24 (internal quotation marks omitted). As Apple has explained, the technical assistance
25 sought here requires vastly more than simply pressing a “few buttons.”

26 The government has every right to reasonably involve the public in the law
27 enforcement process. Indeed, each year Apple complies with thousands of lawful
28 requests for data and information by law enforcement, and on many occasions has

1 extracted data from prior versions of its operating system for the FBI's use. *See* Olle
2 Decl. ¶¶ 15-16. But compelling minimal assistance to surveil or apprehend a criminal
3 (as in most of the cases the government cites), or demanding testimony or production
4 of things that already *exist* (akin to exercising subpoena power), is vastly different, and
5 significantly less intrusive, than conscripting a private company to create something
6 *entirely new* and dangerous. There is simply no parallel or precedent for it.

7 **c. The Government Has Not Demonstrated Apple's Assistance**
8 **Was Necessary To Effectuating The Warrant.**

9 A third party cannot be compelled to assist the government unless the
10 government is authorized to act *and* the third party's participation is imperative. The
11 order in *New York Telephone Co.* satisfied that requirement because the court had
12 authorized surveillance, and "there [was] no conceivable way" to accomplish that
13 surveillance without the company's assistance. 434 U.S. at 175 (noting that FBI had
14 conducted "an exhaustive search" for a way to install a pen register in an undetectable
15 location). The order compelling the phone company's assistance was therefore
16 necessary "to prevent nullification of the court's warrant" and "to put an end to this
17 venture." *Id.* at 174, 175 & n.23; *see also* *Mountain Bell*, 616 F.2d at 1129 (holding
18 that an order compelling a third party to assist with tracing was necessary to carry out a
19 wiretap and halt ongoing criminal activity); *Mich. Bell Telephone Co. v. United States*,
20 565 F.2d 385, 389 (6th Cir. 1977) (concluding that telephone company was "the only
21 entity that c[ould] effectuate the order of the district court to prevent company-owned
22 facilities from being used in violation of both state and federal laws").

23 Here, by contrast, the government has failed to demonstrate that the requested
24 order was absolutely necessary to effectuate the search warrant, including that it
25 exhausted all other avenues for recovering information. Indeed, the FBI foreclosed
26 one such avenue when, without consulting Apple or reviewing its public guidance
27 regarding iOS, the government changed the iCloud password associated with an
28 attacker's account, thereby preventing the phone from initiating an automatic iCloud

1 back-up. *See supra* II.C. Moreover, the government has not made any showing that it
2 sought or received technical assistance from other federal agencies with expertise in
3 digital forensics, which assistance might obviate the need to conscript Apple to create
4 the back door it now seeks. *See* Hanna Decl. Ex. DD at 34–36 [October 26, 2015
5 Transcript] (Judge Orenstein asking the government “to make a representation for
6 purposes of the All Writs Act” as to whether the “entire Government,” including the
7 “intelligence community,” did or did not have the capability to decrypt an iPhone, and
8 the government responding that “federal prosecutors don’t have an obligation to
9 consult the intelligence community in order to investigate crime”). As such, the
10 government has not demonstrated that “there is no conceivable way” to extract data
11 from the phone. *New York Tel. Co.*, 434 U.S. at 174.

12 **3. Other Cases The Government Cites Do Not Support The Type Of** 13 **Compelled Action Sought Here.**

14 The government does not cite a single case remotely approximating the demand
15 it makes here; indeed, its cases only confirm the wild overreach of the Order.

16 The government relies, for example, on cases compelling *a criminal defendant*
17 to take certain actions—specifically, *United States v. Fricosu*, 841 F. Supp. 2d 1232
18 (D. Colo. 2012) and *United States v. Catoggio*, 698 F.3d 64 (2d Cir. 2012) (per
19 curiam)—but those cases say nothing about the propriety of compelling an innocent
20 third party to do so. In *Fricosu* the government moved to require the defendant to
21 produce the “unencrypted contents” of her laptop computer. 841 F. Supp. 2d at 1235.
22 This order placed no undue burden on the defendant because she could access the
23 encrypted contents on her computer, and the court preserved her Fifth Amendment
24 rights by not compelling the password itself, which was testimonial in nature. *See id.*
25 at 1236–38. By contrast, the government’s request here creates an unprecedented
26 burden on Apple and violates Apple’s First Amendment rights against compelled
27 speech, as discussed below. And unlike the compelled creation of a compromised
28 operating system for iOS devices, the order in *Fricosu* merely required the defendant

1 to hand over her own personal files, and thus posed no risk to third parties' privacy or
2 security interests.

3 The government's reliance on *Catoggio*, which involved the seizure of
4 defendant's property, is also inapt. Though the district court had not invoked the All
5 Writs Act, the appellate court cited the Act in affirming the district court's order
6 retaining a convicted defendant's property in anticipation of a restitution order. 698
7 F.3d at 68–69. But whereas courts have uniformly held that the Act enables a court to
8 restrain a convicted defendant's property pending a restitution order, *id.* at 67, no court
9 has ever held that the All Writs Act permits the government to conscript a private
10 company to build software for it.

11 Finally, the government relies on the Ninth Circuit's decision in *Plum Creek*—
12 but that case only serves to illustrate the government's vast overreach under the All
13 Writs Act. There, the Ninth Circuit affirmed the district court's order declining
14 OSHA's request to compel an employer to rescind a company policy forbidding
15 employees from wearing OSHA air-quality and noise-level testing devices, so that
16 OSHA could more efficiently investigate the company's premises. 608 F.2d at 1289–
17 90. The court reasoned that a government agency's interest in conducting an efficient
18 investigation is not grounds for issuing a writ requiring a company to comply with the
19 government's demands. *Id.* at 1290. This was particularly true where OSHA “c[ould]
20 not guarantee that these devices would [not] cause” industry accidents, and the
21 company bore the costs of those accidents. *Id.* at 1289 & n.4 (internal quotation marks
22 omitted). Even though the investigation would take five times as long to complete
23 without the use of the equipment OSHA sought to compel, the court could not compel
24 their use absent a law requiring it. *Id.* at 1289 & n.6. The court held that the All Writs
25 Act “does not give the district court a roving commission to order a party subject to an
26 investigation to accept additional risks at the bidding of OSHA inspectors.” *Id.* at
27 1289. *Plum Creek* thus provides no support for the government's attempt to compel
28 Apple to create new software “when Congress has failed to impose” such a duty on

1 Apple. *Id.* at 1290. Forcing Apple to write software that would create a back door to
2 millions of iOS devices would not only “usurp the legislative function,” *id.*, but also
3 unconstitutionally compel speech and expose Apple iPhone users to exceptional
4 security and privacy risks.

5 **B. The Order Would Violate The First Amendment And The Fifth**
6 **Amendment’s Due Process Clause.**

7 **1. The First Amendment Prohibits The Government From Compelling**
8 **Apple To Create Code**

9 The government asks this Court to command Apple to write software that will
10 neutralize safety features that Apple has built into the iPhone in response to consumer
11 privacy concerns. Order ¶ 2. The code must contain a unique identifier “so that [it]
12 would only load and execute on the SUBJECT DEVICE,” and it must be “signed”
13 cryptographically by Apple using its own proprietary encryption methods.” Ex Parte
14 App. at 5, 7. This amounts to compelled speech and viewpoint discrimination in
15 violation of the First Amendment.

16 Under well-settled law, computer code is treated as speech within the meaning
17 of the First Amendment. *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d
18 429, 449 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *321*
19 *Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1099–1100
20 (N.D. Cal. 2004); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1126 (N.D. Cal.
21 2002); *Bernstein v. Dep’t of State*, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

22 The Supreme Court has made clear that where, as here, the government seeks to
23 *compel* speech, such action triggers First Amendment protections. As the Court
24 observed in *Riley v. Nat’l Fed. of the Blind of N.C., Inc.*, 487 U.S. 781,796 (1988),
25 while “[t]here is certainly some difference between compelled speech and compelled
26 silence, . . . in the context of protected speech, the difference is without constitutional
27 significance.” Compelled speech is a content-based restriction subject to exacting
28 scrutiny, *id.* at 795, 797–98, and so may only be upheld if it is narrowly tailored to

1 obtain a compelling state interest, *see Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622,
2 662 (1994).

3 The government cannot meet this standard here. Apple does not question the
4 government’s legitimate and worthy interest in investigating and prosecuting terrorists,
5 but here the government has produced nothing more than speculation that this iPhone
6 might contain potentially relevant information.²⁶ Hanna Decl. Ex. H [Comey, *Follow*
7 *This Lead*] (“Maybe the phone holds the clue to finding more terrorists. Maybe it
8 doesn’t.”). It is well known that terrorists and other criminals use highly sophisticated
9 encryption techniques and readily available software applications, making it likely that
10 any information on the phone lies behind several other layers of non-Apple encryption.
11 *See* Hanna Decl. Ex. E [Coker, *Tech Savvy*] (noting that the Islamic State has issued to
12 its members a ranking of the 33 most secure communications applications, and “has
13 urged its followers to make use of [one app’s] capability to host encrypted group
14 chats”).

15 Even more problematically, the Court’s Order discriminates on the basis of
16 Apple’s viewpoint. When Apple designed iOS 8, it wrote code that announced the
17 value it placed on data security and the privacy of citizens by omitting a back door that
18 bad actors might exploit. *See, e.g.*, Hanna Decl. Ex. AA [Apple Inc., *Privacy,*
19 *Government Information Requests*]. The government disagrees with this position and
20 asks this Court to compel Apple to write new software that advances its contrary
21 views. This is, in every sense of the term, viewpoint discrimination that violates the

22
23 ²⁶ If the government did have any leads on additional suspects, it is inconceivable that
24 it would have filed pleadings on the public record, blogged, and issued press
25 releases discussing the details of the situation, thereby thwarting its own efforts to
26 apprehend the criminals. *See Douglas Oil Co. of Cal. v. Petrol Stops Nw.*, 441 U.S.
27 211, 218-19 (1979) (“We consistently have recognized that the proper functioning
28 of our grand jury system depends upon the secrecy of grand jury proceedings. . . .
[I]f preindictment proceedings were made public, many prospective witnesses
would be hesitant to come forward voluntarily, knowing that those against whom
they testify would be aware of that testimony. . . . There also would be the risk that
those about to be indicted would flee, or would try to influence individual grand
jurors to vote against indictment.”).

1 First Amendment. *See Members of City Council v. Taxpayers for Vincent*, 466 U.S.
2 789, 804 (1984).

3 Finally, the FBI itself foreclosed what would have likely been a promising and
4 vastly narrower alternative to this unprecedented order: backing up the iPhone to
5 iCloud. Apple has extensively cooperated and assisted law enforcement officials in the
6 San Bernardino investigation, but the FBI inadvertently foreclosed a ready avenue by
7 changing the passcode, which precluded the iCloud back-up option.²⁷

8 To avoid the serious First Amendment concerns that the government’s request to
9 compel speech presents, this Court should vacate the Order.

10 **2. The Fifth Amendment’s Due Process Clause Prohibits The**
11 **Government From Compelling Apple To Create The Request Code**

12 In addition to violating the First Amendment, the government’s requested order,
13 by conscripting a private party with an extraordinarily attenuated connection to the
14 crime to do the government’s bidding in a way that is statutorily unauthorized, highly
15 burdensome, and contrary to the party’s core principles, violates Apple’s substantive
16 due process right to be free from “arbitrary deprivation of [its] liberty by
17 government.” *Costanich v. Dep’t of Soc. & Health Servs.*, 627 F.3d 1101, 1110 (9th
18 Cir. 2010) (citation omitted); *see also, e.g., Cnty. of Sacramento v. Lewis*, 523 U.S.
19 833, 845-46 (1998) (“We have emphasized time and again that ‘[t]he touchstone of
20 due process is protection of the individual against arbitrary action of government,’ . . .
21 [including] the exercise of power without any reasonable justification in the service of
22 a legitimate governmental objective.” (citations omitted)); *cf. id.* at 850 (“Rules of due
23 process are not . . . subject to mechanical application in unfamiliar territory.”).

24
25
26 ²⁷ Hanna Decl. Ex. BB [John Paczkowski and Chris Geidner, *FBI Admits It Urged*
27 *Change Of Apple ID Password For Terrorist’s iPhone*, BuzzFeed News (updated
28 Feb. 21, 2016 2:01 AM)]; Hanna Decl. Ex. CC [Ellen Nakashima and Mark
Berman, *FBI Asked San Bernardino to Reset the Password for Shooter’s Phone*
Backup, Wash. Post (Feb. 20, 2016)].

IV. CONCLUSION

Apple has great respect for the professionals at the Department of Justice and FBI, and it believes their intentions are good. Moreover, Apple has profound sympathy for the innocent victims of the attack and their families. However, while the government's desire to maximize security is laudable, the decision of how to do so while also protecting other vital interests, such as personal safety and privacy, is for American citizens to make through the democratic process. Indeed, examples abound of society opting *not* to pay the price for increased and more efficient enforcement of criminal laws. For example, society does not tolerate violations of the Fifth Amendment privilege against self-incrimination, even though more criminals would be convicted if the government could compel their confessions. Nor does society tolerate violations of the Fourth Amendment, even though the government could more easily obtain critical evidence if given free rein to conduct warrantless searches and seizures. At every level of our legal system—from the Constitution,²⁸ to our statutes,²⁹ common law,³⁰ rules,³¹ and even the Department of Justice's own policies³²—society has acted to preserve certain rights at the expense of burdening law enforcement's interest in investigating crimes and bringing criminals to justice. Society is still debating the important privacy and security issues posed by this case. The government's desire to leave no stone unturned, however well intentioned, does not authorize it to cut off debate and impose its views on society.

²⁸ *See, e.g.*, U.S. Const. amend. IV (limitations on searches and seizures), amend. V (limitations on charging; prohibition on compelling testimony of accused).

²⁹ *See, e.g.*, 18 U.S.C. § 3282 (prohibition on prosecuting crimes more than five years' old), CALEA (limitations on ability to intercept communications).

³⁰ *E.g.*, attorney-client privilege, spousal privilege, and reporter's privilege, and priest-penitent privilege, all of which limit the government's ability to obtain evidence.

³¹ *See, e.g.*, Fed. R. Evid. 404 (limitations on use of character evidence), 802 (limitations on use of hearsay).

³² *See, e.g.*, U.S. Attorneys' Manual §§ 9-13-200 (limitations on communicating with witnesses represented by counsel), 9-13.400 (limitations on subpoenaing news media), 9-13-410 (limitations on subpoenaing attorneys), 9-13-420 (limitations on searches of attorneys' offices).

1 Dated: February 25, 2016

Respectfully submitted,

2 GIBSON, DUNN & CRUTCHER LLP

3 By: /s/ Theodore J. Boutrous Jr.

4 Theodore J. Boutrous, Jr.

5 Theodore J. Boutrous, Jr.

6 Nicola T. Hanna

Eric D. Vandavelde

7 Gibson, Dunn & Crutcher LLP

333 South Grand Avenue

8 Los Angeles, CA 90071-3197

Telephone: 213.229.7000

9 Facsimile: 213.229.7520

10 Theodore B. Olson

11 Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.

12 Washington, DC 20036-5306

13 Telephone: 202.955.8500

14 Facsimile: 202.467.0539

15 Marc J. Zwillinger *

Jeffrey G. Landis *

ZwillGen PLLC

16 1900 M Street N.W., Suite 250

17 Washington, D.C. 20036

Telephone: 202.706.5202

18 Facsimile: 202.706.5298

**Pro Hac Vice* Admission Pending

19 *Attorneys for Apple Inc.*

1 THEODORE J. BOUTROUS JR., SBN 132099
tboutrous@gibsondunn.com
2 NICOLA T. HANNA, SBN 130694
nhanna@gibsondunn.com
3 ERIC D. VANDEVELDE, SBN 240699
evandeveld@ibsondunn.com
4 GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
5 Los Angeles, CA 90071-3197
Telephone: 213.229.7000
6 Facsimile: 213.229.7520

7 THEODORE B. OLSON, SBN 38137
tolson@gibsondunn.com
8 1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
9 Telephone: 202.955.8500
Facsimile: 202.467.0539

10 MARC J. ZWILLINGER*
11 marc@zwillgen.com
JEFFREY G. LANDIS*
12 jeff@zwillgen.com
ZWILLGEN PLLC
13 1900 M Street N.W., Suite 250
Washington, D.C. 20036
14 Telephone: 202.706.5202
Facsimile: 202.706.5298
15 *Pro Hac Vice Admission Pending

16 UNITED STATES DISTRICT COURT
17 CENTRAL DISTRICT OF CALIFORNIA
18 EASTERN DIVISION

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

ED No. CM 16-10 (SP)

**DECLARATION OF ERIK
NEUENSCHWANDER IN SUPPORT
OF APPLE INC'S MOTION TO
VACATE ORDER COMPELLING
APPLE INC. TO ASSIST AGENTS IN
SEARCH, AND OPPOSITION TO
GOVERNMENT'S MOTION TO
COMPEL ASSISTANCE**

Hearing:

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

1 I, Erik Neuenschwander, declare:

2 1. I am over the age of eighteen years and am competent and authorized to
3 make this declaration. I have personal knowledge of the facts set forth below except as
4 to any facts set forth upon information and belief. As to those facts, I believe them to
5 be true. If called as a witness, I would and could testify to the statements and facts
6 contained herein, all of which are true and accurate to the best of my knowledge and
7 belief.

8 2. I have reviewed the Government's *Ex Parte* Application for Order
9 Compelling Apple Inc. to Assist Agents in Search, the Memorandum of Points and
10 Authorities in support of that application, and the Declaration of Christopher Pluhar. I
11 have also reviewed the Court's February 16, 2016 Order Compelling Apple Inc. to
12 Assist Agents in Search and the Government's February 19, 2016 Motion to Compel.

13 3. To the extent Apple Inc. ("Apple") is required to perform the services that
14 the government demands in these documents, I will likely be tasked with planning the
15 project, which would be implemented by multiple engineers and additional Apple
16 personnel across different groups.

17 **Background**

18 4. I have worked for Apple for over eight years, with more than half of that
19 period focused on privacy matters. I am presently Manager of User Privacy. In that
20 role, I am primarily responsible for the privacy design of Apple's products and
21 services. This includes performing ongoing reviews of the privacy impact of various
22 features in, and data collected by, Apple products and services (in coordination with a
23 team of Apple engineers under my supervision), coordinating with Apple's global
24 privacy policy organization and, with the legal department, coordinating outreach and
25 communications with regulators and standards bodies. Prior to becoming User Privacy
26 Manager, my title was Product Security and Privacy Manager, a role I held for four
27 years.

1 5. Prior to joining Apple in 2007, I spent over four years at Microsoft
2 Corporation as a Program Manager.

3 6. I attended Stanford University where I obtained both a Bachelor of
4 Science degree in Symbolic Systems and a Master of Arts degree in Philosophy.
5 During the time I was getting my Master of Arts degree, I was also a teaching fellow at
6 Stanford, teaching classes in Computer Science including C++ and Object-Oriented
7 Programming.

8 7. All told, I have spent the majority of the last 13 years focusing on
9 software engineering, with a significant focus on privacy and security dating back
10 more than twenty years.

11 **Overview of Security of Apple's Devices**

12 8. In September 2014, Apple announced that iPhones and other devices
13 operating Apple's then-newest operating system, iOS 8, would include hardware- and
14 software-based encryption of the password-protected contents of the devices by
15 default. These protections are designed to prevent anyone without the passcode from
16 accessing stored data on the device.

17 9. When a user sets up an iPhone, the user designates a device passcode,
18 consisting of four, six, or more alphanumeric characters. This passcode is part of the
19 encryption for files with certain classes of protection. The stronger the user passcode
20 is, the stronger the encryption becomes. On iPhones running iOS 8 or newer operating
21 systems, the major types of user data, including messages, photos, contacts, email,
22 notes, and calendar data all are encrypted with keys protected by a key derived from
23 the user-chosen passcode. The end result is a person must know that passcode to read
24 this data.

25 10. To prevent "brute-force" attempts to determine the passcode by
26 submitting multiple guesses in rapid succession, iOS includes a variety of safeguards.

27 11. One of these safeguards is referred to as a "large iteration count." This
28 safeguard functions to slow attempts to unlock an iPhone by increasing the

1 computational burden of each attempt. The iteration count is calibrated so that one
2 attempt to unlock an iPhone takes approximately 80 milliseconds.

3 12. As another safeguard, Apple imposes time delays, including one which
4 escalates after the entry of invalid passcodes to deter anyone attempting to improperly
5 access a phone by guessing the passcode. After enough consecutive incorrect attempts
6 to enter the passcode, the time delay is set to an infinite value, such that the device will
7 refuse to accept any further passcode entries. There is also a user-configurable setting
8 (“Erase Data”) which automatically deletes keys needed to read encrypted data after
9 ten consecutive incorrect attempts. Even when this setting is disabled, however, the
10 infinite delay limits the number of passcode attempts.

11 13. A further safeguard for iOS devices is the creation of a Unique ID
12 (“UID”) for every device during fabrication, which is not accessible to the operating
13 system or stored by Apple. When the decryption key for a device is being generated,
14 the user-chosen passcode is entangled with that device’s UID. This means that data is
15 protected with a key cryptographically tied to a given device, and consequently iOS is
16 designed to require passcode validation (and therefore any attempted brute-force
17 attack) be performed on the physical device itself.

18 14. Each of the features described above is present in the operating system on
19 the device in question in this matter.

20 **The Government’s Request**

21 15. As I understand it, the government is demanding that Apple build for the
22 FBI a version of Apple’s iPhone operating system that does not currently exist, that
23 Apple would not otherwise build, and that can be used to defeat the above-referenced
24 security measures on Apple devices such as the device at issue here. I will refer to this
25 operating system as GovtOS.

26 16. Specifically, I understand that the government wants GovtOS to (1)
27 bypass or disable the Erase Data function on the device, whether or not it has been
28 enabled; (2) enable the FBI to submit passcodes to the device electronically as opposed

1 to manually, which is how Apple devices are now designed to accept passcodes; and
2 (3) ensure that when the FBI submits passcodes to the device electronically, software
3 running on the device will not introduce additional time delays between passcode
4 attempts beyond what is incurred by Apple's hardware.

5 17. The government wants GovtOS to load and run from Random Access
6 Memory ("RAM"), and not modify the operating system on the actual phone, the user
7 data partition, or the system partition on the device's flash memory.

8 18. I understand that the government wants Apple to cryptographically sign
9 GovtOS to represent that it is a legitimate Apple product, and then load it onto the
10 device in question so that the government can attempt to brute-force hack the device,
11 either directly or remotely.

12 19. Apple's current iPhone operating systems designed for consumer
13 interaction do not run in RAM, but are installed on the device itself. To make them
14 run in RAM, Apple would have to make substantial reductions in the size and
15 complexity of the code.

16 20. Apple's current consumer operating systems do not allow for electronic
17 input of a passcode.

18 **Creating and Testing the Operating System**

19 21. The government is asking Apple to do something that, to my knowledge,
20 Apple has never done before. Accordingly, it is difficult to accurately predict exactly
21 the work such a project would entail and how long it would take.

22 22. I would estimate that the design, creation, validation, and deployment of
23 GovtOS would necessitate between six and ten Apple engineers and employees
24 dedicating a very substantial portion of their time for two weeks at a minimum, and
25 likely as many as four weeks. This includes, in addition to myself, at least two
26 engineers from Apple's core operating system group, a quality assurance engineer, a
27 project manager, and either a document writer or a tool writer (depending on whether
28 Apple is writing the tool to submit passcodes electronically or a protocol so that the

1 government can do so). This does not include the other personnel who would support
2 those individuals.

3 23. These individuals would otherwise be performing engineering tasks
4 related to Apple's products. New employees could not be hired to perform these tasks,
5 as they would have insufficient knowledge of Apple's software and design protocols to
6 be effective in designing and coding the software without significant training.

7 24. The first step in the process would be for Apple to design and create an
8 operating system that can accomplish what the government wants. No such operating
9 system currently exists with this combination of features. Moreover, Apple cannot
10 simply remove a few lines of code from existing operating systems. Rather, Apple will
11 need to design and implement untested functionality in order to allow the capability to
12 enter passcodes into the device electronically in the manner that the government
13 describes.

14 25. Creating the ability to enter passcodes into a device electronically with no
15 software-imposed delays would entail modifying existing code to remove delays as
16 well as writing new code that manages a connection to another device and, using a
17 communications protocol that would also have to be designed, allows the other device
18 to submit test passcodes and receive and process the result of those tests. The means
19 for establishing such connection could include Wi-Fi, Bluetooth, or direct cable
20 connection.

21 26. Apple will also need to either (1) develop and prepare detailed
22 documentation for the above protocol to enable the FBI to build a brute-force tool that
23 is able to interface with the device to input passcode attempts, or (2) design, develop
24 and prepare documentation for such a tool itself. Further, if the tool is utilized
25 remotely (rather than at a secure Apple facility), Apple will also have to develop
26 procedures to encrypt, validate, and input into the device communications from the
27 FBI.

28

1 system to bypass the device's security features will not inadvertently destroy or alter
2 the user data on the data partition.

3 33. To the extent during the quality assurance and security testing process
4 problems are identified (which is almost always the case), solutions will need to be
5 developed and re-coded into the new operating system. Once such solutions are
6 inputted, the quality assurance and security testing process will begin anew.

7 34. The entire quality assurance and security testing process would also likely
8 be logged, recorded, and preserved in case Apple's methodology is ever questioned,
9 for example in court.

10 **Deploying the Operating System on the Subject Device**

11 35. Once the new operating system is created and validated, it will need to be
12 deployed on to the subject device.

13 36. The deployment will need to be done at an Apple facility. That is because
14 GovtOS is not intended to run on any consumer device except with the validation of
15 Apple in circumstances where due process is followed. In addition, simply delivering
16 the operating system to the government would impose upon the government full
17 responsibility for securing it from hackers and others looking to get their hands on it.

18 37. Once GovtOS is created, Apple will need to set up a secure, isolated
19 physical facility where the FBI's passcode testing can be conducted without interfering
20 with the investigation or disrupting Apple's operations. At that facility, the FBI can
21 then connect the device to a computer equipped with the passcode testing tool and
22 conduct its tests for as long as that process takes. At the conclusion of the FBI's
23 testing, whether or not successful, the subject device will need to be restarted so that
24 GovtOS is erased from the device's memory, and Apple can confirm that this sensitive
25 software does not ever leave its facility.

26 38. The deployment steps for a particular device outlined above will require
27 additional time beyond the creation and testing of GovtOS, likely at least a day (not
28 including FBI time spent at Apple's facility testing passcodes).

1 **Destroying or Securing the Operating System**

2 39. The government’s papers suggest that once deployment of GovtOS is
3 completed and the government (presumably) accesses the device, Apple can simply
4 “destroy” GovtOS.

5 40. The government suggests that this would reduce or eliminate any risk of
6 misuse of the new operating system, including potential use on a device other than the
7 device at issue here. I believe this to be a fundamentally flawed premise.

8 41. The virtual world is not like the physical world. When you destroy
9 something in the physical world, the effort to recreate it is roughly equivalent to the
10 effort required to create it in the first place. When you create something in the virtual
11 world, the process of creating an exact and perfect copy is as easy as a computer key
12 stroke because the underlying code is persistent.

13 42. Even if the underlying computer code is completely eradicated from
14 Apple’s servers so as to be irretrievable, the person who created the destroyed code
15 would have spent the time and effort to solve the software design, coding and
16 implementation challenges. This process could be replicated. Thus, GovtOS would
17 not be truly destroyed.

18 43. Moreover, even if Apple were able to truly destroy the actual operating
19 system and the underlying code (which I believe to be an unrealistic proposition), it
20 would presumably need to maintain the records and logs of the processes it used to
21 create, validate, and deploy GovtOS in case Apple’s methods ever need to be
22 defended, for example in court. The government, or anyone else, could use such
23 records and logs as a roadmap to recreate Apple’s methodology, even if the operating
24 system and underlying code no longer exist.

25 44. All told, I would estimate that the process of designing, creating,
26 validating, deploying GovtOS would take two to four weeks, with additional time
27 spent on eradication (assuming that is possible).

28

1 **Burden of Repeated Requests**

2 45. Given the complexity of designing, creating, validating, deploying, and
3 eradicating a bespoke operating system such as the government demands, the burden
4 on Apple will increase significantly as the number of requests to Apple increase.

5 46. For example, if Apple receives three orders a week similar to the one here
6 from around the United States, the entire process described above—writing, validating,
7 executing, and then completely destroying the code—will have to happen three times
8 every week, week in and week out. Each such commissioned operating system will
9 need to be tailored to the specific combination of hardware and operating system
10 running on the relevant device.

11 47. The other alternative would be for Apple to maintain custody of GovtOS.
12 Doing that creates an entirely different set of burdens. If a purpose-built operating
13 system such as the one the government seeks here got into the wrong hands it would
14 open a significant new avenue of attack, undermining the security protections that
15 Apple spent years developing to protect its customers.

16 48. Apple would thus need to impose the same level of security protections
17 around GovtOS (as well as the source code used to create it and records and logs
18 document its creation, validation, and deployment) that Apple now employs for its
19 most sensitive trade secrets.

20 49. These measures would need to be maintained for as long as Apple was
21 being required to create and deploy specialized operating systems like those demanded
22 here.

23 **Novelty of the Government's Request**

24 50. What the government is requesting Apple do is not something that Apple
25 has ever done before or would otherwise do.

26 51. Apple does not create operating systems the purpose of which is to defeat
27 the security measures Apple specifically designs in to its products.
28

1 52. Apple does not build bespoke operating systems that are only intended to
2 be installed a single time.

3 53. Apple does not create operating systems built to third-party specifications
4 provided uniquely to Apple.

5 **Alternative Ways of Obtaining Information from the Device**

6 54. There are several other ways the government could have potentially
7 obtained any data stored on the subject device.

8 55. I understand that the subject device was provided to the user by his
9 employer, the San Bernardino County Public Health Department (“SBCPHD”), which
10 owned the device.

11 56. The FBI would likely have been able to clear the passcode lock on the
12 device without assistance from Apple had the SBCPHD required that Mobile Device
13 Manager (“MDM”) be installed and activated on the device before giving it to their
14 employees.

15 57. MDM is an Apple feature that allows employers to exercise control over
16 devices used by employees, whether those devices are owned by the employer and
17 provided to the employees or are the employees’ own devices. Using MDM,
18 employers can wirelessly configure and update settings, monitor policy compliance,
19 deploy apps and books, and remotely wipe or lock managed corporate devices.

20 58. Administrative commands available to employers using MDM include
21 changing configuration settings automatically without user interaction and clearing the
22 passcode lock so users can reset forgotten passwords. Had SBCPHD employed MDM
23 in a way that allowed it do those things, SBCHD could simply clear the passcode lock
24 for the government and/or turn off the Erase Data feature for the government.

25 59. The government may also have been able to obtain the latest data from
26 the device through iCloud backup had the FBI not instructed the SBCPHD to change
27 the iCloud password associated with the account.

28

1 THEODORE J. BOUTROUS JR., SBN 132099
tboutrous@gibsondunn.com
2 NICOLA T. HANNA, SBN 130694
nhanna@gibsondunn.com
3 ERIC D. VANDEVELDE, SBN 240699
evandeveld@ibsondunn.com
4 GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
5 Los Angeles, CA 90071-3197
Telephone: 213.229.7000
6 Facsimile: 213.229.7520

7 THEODORE B. OLSON, SBN 38137
tolson@gibsondunn.com
8 1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
9 Telephone: 202.955.8500
Facsimile: 202.467.0539

10 MARC J. ZWILLINGER*
11 marc@zwillgen.com
JEFFREY G. LANDIS*
12 jeff@zwillgen.com
ZWILLGEN PLLC
13 1900 M Street N.W., Suite 250
Washington, D.C. 20036
14 Telephone: 202.706.5202
Facsimile: 202.706.5298
15 *Pro Hac Vice Admission Pending

16 Attorneys for Apple Inc.

17 UNITED STATES DISTRICT COURT
18 CENTRAL DISTRICT OF CALIFORNIA
19 EASTERN DIVISION

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

ED No. CM 16-10 (SP)

**DECLARATION OF LISA OLLE IN
SUPPORT OF APPLE INC'S
MOTION TO VACATE ORDER
COMPELLING APPLE INC. TO
ASSIST AGENTS IN SEARCH, AND
OPPOSITION TO GOVERNMENT'S
MOTION TO COMPEL ASSISTANCE**

Hearing:

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

1 I, Lisa Olle, declare:

2 1. I am over the age of eighteen years and am competent and authorized to
3 make this declaration. I have personal knowledge of the facts set forth below. If
4 called as a witness, I would and could testify to the statements and facts contained
5 herein, all of which are true and accurate to the best of my knowledge and belief.

6 2. I have worked as an attorney at Apple for more than eight years. Prior to
7 Apple, I worked as an attorney at Perkins Coie LLP. My current title is Manager,
8 Global Privacy & Law Enforcement Compliance Team. My responsibilities include
9 overseeing Apple's response to legal requests for customer data that Apple receives
10 from international, federal, state, and local law enforcement agencies.

11 3. I attended University of California, Berkeley, where I obtained a Bachelor
12 of Arts degree in Legal Studies and attended University of California, Boalt Hall
13 School of Law, where I obtained a Juris Doctor.

14 4. I oversaw Apple's response to the legal requests that Apple received
15 related to the December 2, 2015 shooting in San Bernardino, California.

16 5. On Saturday, December 5, 2015, Apple's emergency 24/7 call center
17 received a call at approximately 2:46 a.m. PST requesting information relating to the
18 case. Throughout that day, Apple employees were in regular communication with the
19 FBI regarding its investigation. The same day, Apple received legal process seeking
20 customer or subscriber information regarding three names and nine specific accounts.
21 In response to that request, Apple made two productions of information that same day.

22 6. Throughout the investigation, I and other Apple representatives, including
23 a senior engineer, continually made ourselves available to the government, on a 24/7
24 basis, participating in teleconferences, providing technical assistance, answering
25 questions from the FBI, and suggesting potential alternatives for the government to
26 attempt to obtain data from the Subject Device.

27 7. On Sunday, December 6, 2015, Apple received a search warrant for
28 information relating to three accounts, including, but not limited to, account

1 information, emails, and messages, associated with the accounts. In response to that
2 search warrant, Apple provided the government with information in Apple's
3 possession that same day.

4 8. On Wednesday, December 16, 2015, Apple received legal process seeking
5 customer or subscriber information regarding one name and seven specific accounts.
6 In response, Apple provided the government with information in Apple's possession
7 that same day.

8 9. On Friday, January 22, 2016, Apple received a search warrant for the
9 iCloud account related to the Subject Device for the same types of information as in
10 the previous warrant. In response, Apple provided the government with information in
11 Apple's possession on Tuesday, January 26, 2016.

12 10. I have reviewed the Government's *Ex Parte* Application for Order
13 Compelling Apple Inc. to Assist Agents in Search, the Memorandum of Points and
14 Authorities in support of that application, and the Declaration of Christopher Pluhar. I
15 have also reviewed the Court's February 16, 2016 Order Compelling Apple Inc. to
16 Assist Agents in Search and the Government's February 19, 2016 Motion to Compel.

17 11. The Court's February 16, 2016 Order granted Apple the opportunity to
18 present information to the Court regarding the government's request, including the
19 burden of providing the services the government seeks.

20 12. In addition to the technical burden of designing, creating, validating,
21 deploying, and eradicating (or maintaining) an operating system such as the
22 government seeks here, there would be significant additional burdens placed on
23 Apple's law enforcement compliance team.

24 13. Just by way of a few examples, for each device, the law enforcement
25 compliance team would need to arrange to receive, safeguard and deliver the device to
26 the Apple engineers responsible for creating and deploying the operating system. The
27 law enforcement compliance team would also need to preserve and log the chain of
28 custody for the device the entire time it was in Apple's possession. Once the operating

1 system was created and deployed on the device, someone in the law enforcement
2 compliance group would then need to liaise with the relevant law enforcement agency
3 to create the ability for that agency to submit passcodes to the “hacked” device. Based
4 on past experience, this will likely involve technical escalations where Apple
5 personnel will need to provide law enforcement with technical guidance and assistance
6 regarding how to submit passcodes to the device. Once law enforcement
7 (presumably) gains access to the relevant device, the Apple law enforcement
8 compliance team would then need to transmit any data on the device, and/or the device
9 itself to law enforcement.

10 14. I believe that Apple would likely create one or two secure facilities with
11 security measures akin to those used in a Sensitive Compartmented Information
12 Facility (“SCIF”), where all work on a device would need to be performed and the
13 device would need to be stored. Access to such facilities would need to be tightly
14 controlled and monitored around the clock.

15 15. Each year Apple complies with thousands of lawful requests for data and
16 information from international, federal, state, and local law enforcement agencies.

17 16. Given my background and experience, I believe that if Apple were
18 required to comply with the order in this case, it would receive similar orders from
19 other law enforcement agencies, and Apple would need to hire people whose sole
20 function would be to assist with processing and effectuating such orders. These
21 people would have no other necessary business or operations function at Apple. They
22 would likely include paralegals, and engineers or forensic specialists who were
23 dedicated full time to preparing for and testifying at trials and hearings. This would be
24 in addition to whatever additional personnel would be necessary to design, create,

1 validate, deploy, and eradicate (or maintain and protect) the operating system itself.

2
3 I declare under penalty of perjury under the laws of the United States of
4 America that the foregoing is true and correct.

5 Executed this 25th day of February 2016 in Sunnyvale, California.

6
7 By: *Lisa Olle*
8 Lisa Olle
9 Manager, Global Privacy & Law
10 Enforcement Compliance Team

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
Apple Inc.