THEODORE J. BOUTROUS JR., SBN 132099
tboutrous@gibsondunn.com
NICOLA T. HANNA, SBN 130694
nhanna@gibsondunn.com
ERIC D. VANDEVELDE, SBN –0699
evandevelde@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

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

MARC J. ZWILLINGER*
marc@zwillgen.com
JEFFFREY G. LANDIS*
jeff@zwillgen.com
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.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	ED No. CM 16-10 (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

Apple Inc. ("Apple"), by and through its counsel of record, hereby files this Motion to Vacate the Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to the Government's Motion to Compel Assistance.

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

Dated: February 25, 2016

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

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

Theodore J. Boutrous, Jr.
Nicola T. Hanna
Eric D. Vandevelde
Gibson, Dunn & Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

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

Marc J. Zwillinger *
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

Page

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 10

D. The Government's *Ex Parte* Application Under The All Writs Act, And This Court's Order 11

E. The Resources And Effort Required To Develop The Software Demanded By The Government 13

III. ARGUMENT 14

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

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. *New York Telephone Co.* 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 20

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. 30

B. The Order Would Violate The First Amendment And The Fifth Amendment's Due Process Clause. 32

1. The First Amendment Prohibits The Government From Compelling Apple To Create Code 32

TABLE OF CONTENTS
(Continued)

Page

2. The Fifth Amendment's Due Process Clause Prohibits The Government From Compelling Apple To Create The Request Code 34

IV. CONCLUSION 35

TABLE OF AUTHORITIES

Page(s)

Cases

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

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

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

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

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

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

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

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

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

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

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

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

TABLE OF AUTHORITIES
(Continued)

Page(s)

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)

Page(s)

Pa. Bureau of Corr. v. U.S. Marshals Serv.,
474 U.S. 34 (1985) 15

Pipe Trades Council, U.A. Loc. 159 v. Underground Contractors Ass'n,
835 F.2d 1275 (9th Cir. 1987) 5

Plaut v. Spendthrift Farm, Inc.,
514 U.S. 211 (1995) 18

Plum Creek Lumber Co. v. Hutton,
608 F.2d 1283 (9th Cir. 1979) 1, 14, 15, 31, 32

Quon v. Arch Wireless Operating Co., Inc.,
529 F.3d 892 (9th Cir. 2008) 17

Riley v. California,
134 S. Ct. 2473 (2014) 25

Riley v. Nat'l Fed. of the Blind of N.C., Inc.,
487 U.S. 781,796 (1988) 32

Saldana v. Occidental Petroleum Corp.,
774 F.3d 544 (9th Cir. 2014) (per curiam) 19

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,
No. ED 15-0451M (Feb. 16, 2016), Dkt. 19 .... 12, 22, 31

State v. Underdahl,
767 N.W.2d 677 (Minn. 2009) 24

Turner Broad. Sys., Inc. v. FCC,
512 U.S. 622 (1994) 33

United States v. Budziak,
697 F.3d 1105 (9th Cir. 2012) 24

United States v. Cameron,
699 F.3d 621 (1st Cir. 2012) 26

United States v. Catoggio,
698 F.3d 64 (2d Cir. 2012) (per curiam) 30

TABLE OF AUTHORITIES
(Continued)

Page(s)

United States v. Cooper,
983 F.2d 928 (9th Cir. 1993) 24

United States v. Elcom Ltd.,
203 F. Supp. 2d 1111 (N.D. Cal. 2002)....................32

United States v. Fricosu,
841 F. Supp. 2d 1232 (D. Colo. 2012) 30

United States v. Hall,
583 F. Supp. 717 (E.D. Va. 1984) 21, 23, 27

United States v. Navarro,
No. 13-CR-5525 (W.D. Wash. Nov. 13, 2013), ECF No. 39....................28

United States v. New York Telephone Co.,
434 U.S. 159 (1977)....................20, 21, 22, 29, 30

Universal City Studios, Inc. v. Corley,
273 F.3d 429 (2d Cir. 2001) 32

Vieth v. Jubelirer,
541 U.S. 267 (2004) (plurality opinion)....................19

Xi v. INS,
298 F.3d 832 (9th Cir. 2002) 19

Youngstown Sheet & Tube Co. v. Sawyer,
343 U.S. 579 (1952)....................18

Statutes

18 U.S.C. § 2518(4) 17

18 U.S.C. § 3282....................35

28 U.S.C. § 1651....................11, 15, 19

47 U.S.C. § 1001....................8, 17

47 U.S.C. § 1002....................8, 16, 17

TABLE OF AUTHORITIES
(Continued)

Page(s)

Other Authorities

Apple Inc., *A Message to Our Customers* (Feb. 16, 2016) 3, 22

Apple Inc. and Apple Distrib. Int'l, Written Evidence (IPB0093), (Dec. 21, 2015) 7

Apple Inc., *iCloud: Back up your iOS device to iCloud*....................................11

Apple Inc., *iOS Security: iOS 9.0 or later* (September 2015). 6

Apple Inc., *Privacy, Government Information Requests*....................................33

Cyrus R. Vance Jr., *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, N.Y. Times (Feb. 18, 2016) 10, 24

Damian Paletta, *How the U.S. Fights Encryption—and Also Helps Develop It*, Wall St. J. (Feb. 22, 2016) 6

Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (July 9, 2015) 1

Ellen Nakashima and Mark Berman, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, Wash. Post (Feb. 20, 2016) 34

Ellen Nakashima, *Proposal Seeks to Fine Tech Companies for Noncompliance with Wiretap Orders*, Wash. Post (Apr. 28, 2013)....................................9

FBI, Operational Technology, *Going Dark Issue* (last visited Feb. 23, 2016) 4, 7

Gen. Michael Hayden Gives an Update on the Cyberwar, 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

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

James Comey, *Encryption, Public Safety, and "Going Dark,"* 4

TABLE OF AUTHORITIES
(Continued)

Page(s)

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

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

TABLE OF AUTHORITIES (Continued)

Page(s)

Rules

Fed. R. Evid. 404 35

Fed. R. Evid. 702 24

Constitutional Provisions

U.S. Const. amend. I 32

U.S. Const. amend. IV 35

U.S. Const. amend. V 34

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

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

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

[1] *See, e.g.*, Hanna Decl. Ex. A [Ellen Nakashima, *Hacks of OPM Databases 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).

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

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

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

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

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

[2] Hanna Decl. Ex. B [Letter to Court, *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] *E.g.*, Hanna Decl. Ex. C [Seung Lee, *The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories*, Newsweek (Feb. 19, 2016)] (Cyrus Vance, Manhattan District Attorney stating that he has "155 to 160" devices that he would like to access, while officials in Sacramento have "well over 100" devices 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").

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

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

As FBI Director James Comey expressly recognized:

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

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

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

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

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

II. BACKGROUND

A. Apple's Industry-Leading Device Security.

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

[5] The government filed its motion to compel notwithstanding the Court allowing an eight-day period within which Apple could challenge the order compelling assistance, Apple's express indication during the parties' February 18 status conference that it intended to seek relief from the order, the Court's entry of a briefing schedule to permit the parties to address the validity of the order, and the Court's own skepticism about the utility of such a motion. That skepticism proved warranted. Only three pages into the government's 25-page motion, it concedes the motion is "not legally necessary." Dkt. 1 at 3 n.3. Nor could the government claim otherwise, as the motion—substantial portions of which appear to have been cut and pasted from the government's *ex parte* application—seeks no relief beyond that contemplated by the order compelling assistance. Because the government's 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)

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

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

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

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

(Cont'd from previous page)

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

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

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

As leading former national security officials have made clear, Apple's "resistance to building in a back door" in whatever form it may take is well-justified,

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

[8] *See, e.g.*, Hanna Decl. Ex. L [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)]. 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 about just one iPhone.

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

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

because "the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."[11]

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

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

[12] Following a vigorous lobbying effort led by the FBI for enhanced surveillance and informational-access powers in the digital age, Congress "balance[d] three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies." H.R. Rep. No. 103-827(I), at 13 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3493; *see also id.* at 17, 1994 U.S.C.C.A.N. at 3497 ("[A]s the potential 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).

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

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

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

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

[16] *See* Secure Data Act of 2015, S.135, 114th Cong. (2015) (proposal to prohibit a federal agency from requiring hardware or software manufacturers to design or alter the security functions in their products to allow surveillance, and exempting products used pursuant to CALEA); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015) (same); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015) (same, adding additional amendments to the Foreign Intelligence Surveillance Act of 1978). In fact, just last week, four senior members 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)

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

C. Apple's Substantial Assistance In The Government's Investigation

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

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

(Cont'd from previous page)

"United States government is actively engaged with private companies to ensure 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.").

[18] *See* Hanna Decl. Ex. T [James Comey, *Director Discusses Encryption, Patriot Act Provisions*, (May 20, 2015)]. Even Manhattan District Attorney Cyrus Vance, Jr., who is eager to see the government prevail here, has acknowledged that these issues 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. 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 States Congress is going to have to step in here . . . We need to look at this with independent eyes. And I believe Congress ultimately is going to have to make the 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)].

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

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

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

On February 16, 2016, the government filed an *ex parte* application and proposed order asking the Court to compel Apple to assist in the government's investigation under the authority of the All Writs Act, codified at 28 U.S.C. § 1651.[22]

[21] In its motion to compel, filed February 19 with this Court, the government sought to shift the blame to the "owner" (San Bernardino County) in describing who changed the password and why it allegedly has no other viable alternatives besides the creation of a new operating system. Dkt. 1 at 18 n.7. The FBI later issued a 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)].

[22] The government obtained the Order without notice to Apple and without allowing Apple an opportunity to be heard. *See Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950) (recognizing that one of the "'fundamental requisite[s] of due process of law is the opportunity to be heard'") (quoting *Grannis v. Ordean*, 234 U.S. 385, 394 (1914)). But this was not a case where the government needed 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)

With no opposition or other perspectives to consider, the Court granted the government's request and signed the government's proposed order, thereby compelling Apple to create new software that would allow the government to hack into an iPhone 5c used by one of the attackers. Order Compelling Apple Inc. to Assist Agents in Search, *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*, No. ED 15-0451M (Feb. 16, 2016), Dkt. at 19 (the "Order").

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

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

(Cont'd from previous page)

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

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

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

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

Once created, the operating system would need to go through Apple's quality assurance and security testing process. *Id.* ¶ 29. Apple's software ecosystem is incredibly complicated, and changing one feature of an operating system often has ancillary or unanticipated consequences. *Id.* ¶ 30. Thus, quality assurance and security testing would require that the new operating system be tested on multiple devices and validated before being deployed. *Id.* Apple would have to undertake additional testing efforts to confirm and validate that running this newly developed operating system to bypass the device's security features will not inadvertently destroy or alter any user data. *Id.* ¶ 31. To the extent problems are identified (which is almost always the case), solutions would need to be developed and re-coded, and testing would begin anew. *Id.* ¶ 32. As with the development process, the entire quality assurance and security testing process would need to be logged, recorded, and preserved. *Id.* ¶ 33. Once the new custom operating system is created and validated, it would need to be deployed on to the subject device, which would need to be done at an Apple facility. *Id.* ¶¶ 34-35. And if the new operating system has to be destroyed and recreated each time a new order is issued, the burden will multiply. *Id.* ¶¶ 44-45.

III. ARGUMENT

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

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

Congress has never authorized judges to compel innocent third parties to provide decryption services to the FBI. Indeed, Congress has expressly withheld that authority in other contexts, and this issue is currently the subject of a raging national policy debate among members of Congress, the President, the FBI Director, and state and local prosecutors. Moreover, federal courts themselves have *never* recognized an inherent authority to order non-parties to become de facto government agents in ongoing criminal investigations. Because the Order is not grounded in any duly enacted rule or statute, and goes well beyond the very limited powers afforded by Article III of the Constitution and the All Writs Act, it must be vacated.

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

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

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

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

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

> (1) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.
>
> (2) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication 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.

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

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

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

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

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

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

For the courts to use the All Writs Act to expand sub rosa the obligations imposed by CALEA as proposed by the government here would not just exceed the scope of the statute, but it would also violate the separation-of-powers doctrine. Just as the "Congress may not exercise the judicial power to revise final judgments," *Clinton v. Jones*, 520 U.S. 681, 699 (1997) (citing *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211 (1995)), courts may not exercise the legislative power by repurposing statutes to meet the evolving needs of society, *see Clark v. Martinez*, 543 U.S. 371, 391 (2005) (court should "avoid inventing a statute rather than interpreting one") (citation, quotation marks, and alterations omitted); *see also Alzheimer's Inst. of Am. Inc. v. Elan Corp.*, 2013 WL 8744216, at *2 (N.D. Cal. Jan. 31, 2013) (Congress alone has authority "to update" a "technologically antiquated" statute "to address the new and rapidly evolving era of computer and cloud-stored, processed and produced data"). Nor does Congress lose "its exclusive constitutional authority to make laws necessary and proper to carry out the powers vested by the Constitution" in times of crisis (whether real or imagined). *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 588–89 (1952). Because a "decision to rearrange or rewrite [a] statute falls within the legislative, not the judicial prerogative[,]" the All Writs Act cannot possibly be deemed to grant to the courts the extraordinary power the government seeks. *Xi v. INS*, 298 F.3d 832, 839 (9th Cir. 2002).

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

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

2. *New York Telephone Co.* 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.

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

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

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

a. Apple's Connection To The Underlying Case Is "Far Removed" 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

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

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

Further, unlike a telecommunications monopoly, Apple is not a "highly regulated public utility with a duty to serve the public." *New York Telephone Co.*, 434 U.S. at 174; *see also Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities* (*"Mountain Bell"*), 616 F.2d 1122, 1132 (9th Cir. 1980) (discussing *New York Telephone Co.* and noting that its ruling compelling assistance under the All Writs Act relied "[t]o a great extent . . . upon the highly regulated, public nature" of the phone company); *In re Order*, 2015 WL 5920207, at *4–5. Whereas public utilities have no "substantial interest in not providing assistance" to the government, 434 U.S. at 174, and "enjoy a monopoly in an essential area of communications," *Mountain Bell*, 616 F.2d at 1131, Apple is a private company that believes that encryption is crucial to protect the security and privacy interests of citizens who use and store their most personal data on their iPhones, "from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going." Hanna Decl. Ex. D at 1 [Apple Inc., *A Message to Our Customers* (Feb. 16, 2016)].

That Apple "designed, manufactured and sold the SUBJECT DEVICE, and wrote and owns the software that runs the phone," Memorandum of Points and Authorities in Support of Government's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, *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*, No. ED 15-0451M (Feb. 16, 2016), Dkt. 18 at 11 (the "Ex Parte App."), is insufficient to establish the connection mandated by *New York Telephone Co*. The All Writs Act does not allow the government to compel a manufacturer's assistance merely because it has placed a good into the stream of commerce. Apple is no more connected to this phone than General Motors is to a company car used by a fraudster on his daily commute. Moreover, that Apple's software is "licensed, not sold," Ex Parte App. at 5, is "a total red herring," as Judge Orenstein already concluded, Hanna Decl. Ex. DD at 42:4–10 [*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 ("October 26, 2015 Transcript")]. A licensing agreement no more connects Apple to the underlying events than a sale. The license does not permit Apple to invade or control the private data of its customers. It merely limits customers' use and redistribution of Apple's software. Indeed, the government's position has no limits and, if accepted, would eviscerate the "remoteness" factor entirely, as any company that offers products or services to consumers could be conscripted to assist with an investigation, no matter how attenuated their connection to the criminal activity. This is not, and never has been, the law.

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

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

The government's request violates the second requirement—that the Act "must not . . . impose an undue burden"—because the government's unprecedented demand forces Apple to develop new software that destroys the security features that Apple has spent years building. As discussed *supra* in section II.E, no operating system currently exists that can accomplish what the government wants, and any effort to create one would require that Apple write new code, not just disable existing functionality. Neuenschwander Decl. ¶¶ 23-25. Experienced Apple engineers would have to design, create, test, and validate the compromised operating system, using a hyper-secure 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 system itself would have to be tested on multiple devices to ensure that the operating system works and does not alter any data on the device. Neuenschwander Decl. ¶¶ 30-31. All aspects of the development and testing processes would need to be logged and recorded in case Apple's methodology is ever questioned. *Id.* ¶¶ 28, 33.

Moreover, the government's flawed suggestion to delete the program and erase every trace of the activity would not lessen the burden, it would actually increase it since there are hundreds of demands to create and utilize the software waiting in the wings. *Id.* ¶¶ 38-45. If Apple creates new software to open a back door, other federal and state prosecutors—and other governments and agencies—will repeatedly seek orders compelling Apple to use the software to open the back door for tens of thousands of iPhones. Indeed, Manhattan District Attorney Cyrus Vance, Jr., has made clear that the federal and state governments want access to *every* phone in a criminal investigation.[24] *See* Hanna Decl., Ex. Z [(Cyrus R. Vance, Jr., *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, N.Y. Times (Feb. 18, 2016)]; 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"). This enormously intrusive burden—building everything up and tearing it down for each demand by law enforcement—lacks any support in the cases relied on by the government, nor do such cases exist.

[24] Use of the software in criminal prosecutions only exacerbates the risk of disclosure, given that criminal defendants will likely challenge its reliability. *See* Fed. R. Evid. 702 (listing requirements of expert testimony, including that "testimony [be] the product of reliable principles and methods" and "the expert has reliably applied the principles and methods to the facts of the case," all of which a defendant is entitled to challenge); *see also United States v. Budziak*, 697 F.3d 1105, 1111–13 (9th Cir. 2012) (vacating order denying discovery of FBI software); *State v. Underdahl*, 767 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).

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

In addition, compelling Apple to create software in this case will set a dangerous precedent for conscripting Apple and other technology companies to develop technology to do the government's bidding in untold future criminal investigations. If the government can invoke the All Writs Act to compel Apple to create a special operating system that undermines important security measures on the iPhone, it could argue in future cases that the courts should compel Apple to create a version to track the location of suspects, or secretly use the iPhone's microphone and camera to record sound and video. And if it succeeds here against Apple, there is no reason why the government could not deploy its new authority to compel other innocent and unrelated third-parties to do its bidding in the name of law enforcement. For example, under the same legal theories advocated by the government here, the government could argue that it should be permitted to force citizens to do all manner of things "necessary" to assist it in enforcing the laws, like compelling a pharmaceutical company against its will to produce drugs needed to carry out a lethal injection in furtherance of a lawfully issued death warrant,[25] or requiring a journalist to plant a false story in order to help lure out a fugitive, or forcing a software company to insert malicious code in its auto-update process that makes it easier for the government to conduct court-ordered surveillance. Indeed, under the government's formulation, any party whose assistance is deemed "necessary" by the government falls within the ambit of the All Writs Act and can be compelled to do anything the government needs to effectuate a lawful court order. While these sweeping powers might be nice to have from the government's perspective, they simply are not authorized by law and would violate the Constitution.

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

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

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

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

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

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

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

The government has every right to reasonably involve the public in the law enforcement process. Indeed, each year Apple complies with thousands of lawful requests for data and information by law enforcement, and on many occasions has extracted data from prior versions of its operating system for the FBI's use. *See* Olle Decl. ¶¶ 15-16. But compelling minimal assistance to surveil or apprehend a criminal (as in most of the cases the government cites), or demanding testimony or production of things that already *exist* (akin to exercising subpoena power), is vastly different, and significantly less intrusive, than conscripting a private company to create something *entirely new* and dangerous. There is simply no parallel or precedent for it.

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

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

Here, by contrast, the government has failed to demonstrate that the requested order was absolutely necessary to effectuate the search warrant, including that it exhausted all other avenues for recovering information. Indeed, the FBI foreclosed one such avenue when, without consulting Apple or reviewing its public guidance regarding iOS, the government changed the iCloud password associated with an attacker's account, thereby preventing the phone from initiating an automatic iCloud back-up. *See supra* II.C. Moreover, the government has not made any showing that it sought or received technical assistance from other federal agencies with expertise in digital forensics, which assistance might obviate the need to conscript Apple to create the back door it now seeks. *See* Hanna Decl. Ex. DD at 34–36 [October 26, 2015 Transcript] (Judge Orenstein asking the government "to make a representation for purposes of the All Writs Act" as to whether the "entire Government," including the "intelligence community," did or did not have the capability to decrypt an iPhone, and the government responding that "federal prosecutors don't have an obligation to consult the intelligence community in order to investigate crime"). As such, the government has not demonstrated that "there is no conceivable way" to extract data from the phone. *New York Tel. Co.*, 434 U.S. at 174.

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

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

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

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

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

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

B. The Order Would Violate The First Amendment And The Fifth Amendment's Due Process Clause.

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

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

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

The Supreme Court has made clear that where, as here, the government seeks to *compel* speech, such action triggers First Amendment protections. As the Court observed in *Riley v. Nat'l Fed. of the Blind of N.C., Inc.*, 487 U.S. 781,796 (1988), while "[t]here is certainly some difference between compelled speech and compelled silence, . . . in the context of protected speech, the difference is without constitutional significance." Compelled speech is a content-based restriction subject to exacting scrutiny, *id.* at 795, 797–98, and so may only be upheld if it is narrowly tailored to obtain a compelling state interest, *see Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 662 (1994).

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

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

[26] If the government did have any leads on additional suspects, it is inconceivable that it would have filed pleadings on the public record, blogged, and issued press releases discussing the details of the situation, thereby thwarting its own efforts to apprehend the criminals. *See Douglas Oil Co. of Cal. v. Petrol Stops Nw.*, 441 U.S. 211, 218-19 (1979) ("We consistently have recognized that the proper functioning 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.").

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

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

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

2. The Fifth Amendment's Due Process Clause Prohibits The Government From Compelling Apple To Create The Request Code.

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

[27] Hanna Decl. Ex. BB [John Paczkowski and Chris Geidner, *FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone*, BuzzFeed News (updated 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 policies[32]—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).

Dated: February 25, 2016

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

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

Theodore J. Boutrous, Jr.
Nicola T. Hanna
Eric D. Vandevelde
Gibson, Dunn & Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

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

Marc J. Zwillinger *
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.

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

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

MARC J. ZWILLINGER*
marc@zwillgen.com
JEFFFREY G. LANDIS*
jeff@zwillgen.com
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.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	ED No. CM 16-10 (SP) **DECLARATION OF NICOLA T. HANNA 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** **<u>Hearing</u>:** Date: March 22, 2016 Time: 1:00 p.m. Place: Courtroom 3 or 4 Judge: Hon. Sheri Pym

DECLARATION OF NICOLA T. HANNA

I, Nicola T. Hanna, declare as follows:

1. I am an attorney licensed to practice law before this Court. I am a partner in the law firm of Gibson, Dunn & Crutcher LLP, and am one of the attorneys responsible for representing Apple Inc. in the above-captioned matter. I submit this declaration 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. The following facts are true to the best of my knowledge and belief and, if called and sworn as a witness, I could and would testify competently to them.

2. Attached hereto as **Exhibit A** is a true and correct copy of the Washington Post article, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, by Ellen Nakashima, originally published on July 9, 2015, available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. The article was printed on February 23, 2016.

3. Attached hereto as **Exhibit B** is a true and correct copy of the letter to the court filed by Apple Inc. on February 17, 2016 in *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.

4. Attached hereto as **Exhibit C** is a true and correct copy of the Newsweek article, *The Murder Victim Whose Phone Couldn't Be Cracked and Other Apple Encryption Stories*, by Seung Lee, originally published on February 19, 2016, available at http://www.newsweek.com/apple-encryption-crime-428565. The article was printed on February 23, 2016.

5. The Charlie Rose television interview of Cyrus Vance aired on February 18, 2016, and is available at http://www.charlierose.com/watch/60689812.

6. Attached hereto as **Exhibit D** is a true and correct copy of the Apple Inc. document, *A Message to Our Customers*, originally published on February 16, 2016,

available at http://www.apple.com/customer-letter/. The document was printed on February 23, 2016.

7. Attached hereto as **Exhibit E** is a true and correct copy of the Wall Street Journal article, *The Attacks in Paris: Islamic State Teaches Tech Savvy*, by Margaret Coker et al., originally published on November 17, 2015, available at http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824. The article was printed on February 20, 2016.

8. Attached hereto as **Exhibit F** is a true and correct copy of the Federal Bureau of Investigation document, *Going Dark Issue*, available at https://www.fbi.gov/about-us/otd/going-dark-issue. The document was printed on February 23, 2016.

9. Attached hereto as **Exhibit G** is a true and correct copy of the Lawfare blog post, *Encryption, Public Safety, and "Going Dark,"* by James Comey, originally posted on July 6, 2015 at 10:38 AM, available at https://www.lawfareblog.com/encryption-public-safety-and-going-dark. The blog post was printed on February 23, 2016.

10. Attached hereto as **Exhibit H** is a true and correct copy of the Lawfare blog post, *We Could Not Look the Survivors in the Eye if We Did Not Follow This Lead*, by James Comey, originally posted on February 21, 2016 at 9:03 PM, available at https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead. The blog post was printed on February 23, 2016.

11. Attached hereto as **Exhibit I** is a true and correct copy of the Wall Street Journal article, *Gen. Michael Hayden Gives an Update on the Cyberwar*, an interview with John Bussey, originally published on February 9, 2016, available at http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153. The article was printed on February 23, 2016.

12. Attached hereto as **Exhibit J** is a true and correct copy of the Wall Street Journal article, *How the U.S. Fights Encryption—and Also Helps Develop It*, by

Damian Paletta, originally published on February 22, 2016, available at http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096. The article was printed on February 23, 2016.

13. Attached hereto as **Exhibit K** is a true and correct copy of the Apple Inc. document, *iOS Security: iOS 9.0 or later*, originally published in September 2015, available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf. The document was printed on February 23, 2016.

14. Attached hereto as **Exhibit L** is a true and correct copy of the Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption*, by James Comey, originally published on July 8, 2015, available at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. The document was printed on February 23, 2016.

15. Attached hereto as **Exhibit M** is a true and correct copy of the article *The National-Security Needs for Ubiquitous Encryption*, by Susan Landau, Appendix A to the Berkman Center for Internet & Society at Harvard University article *Don't Panic: Making Progress on the 'Going Dark' Debate*, originally published on February 1, 2016, available at https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. The article was printed on February 24, 2016.

16. Attached hereto as **Exhibit N** is a true and correct copy of the written evidence (IPB0093) submitted by Apple Inc. and Apple Distribution International to the Parliament of the United Kingdom on December 21, 2015, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.pdf. The document was printed on February 23, 2016.

17. Attached hereto as **Exhibit O** is a true and correct copy of the Washington Post article, *Why The Fear Of Ubiquitous Data Encryption Is Overblown*, by Mike McConnell et al., originally published on July 28, 2015, available at https://www.washingtonpost.com/ opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html. The article was printed on February 23, 2016.

18. Attached hereto as **Exhibit P** is a true and correct copy of the Washington Post article, *Proposal Seeks To Fine Tech Companies For Noncompliance with Wiretap Orders*, by Ellen Nakashima, originally published on April 28, 2013, available at https://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html. The article was printed on February 23, 2016.

19. Attached hereto as **Exhibit Q** is a true and correct copy of the New America's Open Technology Institute document, *Joint Letter to President Barack Obama*, originally published on May 19, 2015, available at https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf. The document was printed on February 23, 2016.

20. Attached hereto as **Exhibit R** is a true and correct copy of the House Committee on the Judiciary press release, *Senior House Judiciary Committee Democrats Express Concern Over Government Attempts to Undermine Encryption*, by The House Committee on the Judiciary, Democrats, originally published on February 18, 2016, available at http://democrats.judiciary.house.gov/press-release/senior-house-judiciary-committee-democrats-express-concern-over-government-attempts. The press release was printed on February 23, 2016.

21. Attached hereto as **Exhibit S** is a true and correct copy of the *Statement Before the Senate Committee on Homeland Security and Governmental Affairs*, by James Comey, originally published on October 8, 2015, available at

https://www.fbi.gov/news/testimony/threats-to-the-homeland. The document was printed on February 23, 2016.

22. Attached hereto as **Exhibit T** is a true and correct copy of the document *Director Discusses Encryption, Patriot Act Provisions*, by James Comey, originally published on May 20, 2015, available at https://www.fbi.gov/news/news_blog/director-discusses-encryption-patriot-act-provisions. The document was printed on February 23, 2016.

23. Attached hereto as **Exhibit U** is a true and correct copy of the transcript of the radio Interview with Cyrus Vance, *It's Not Just the iPhone Law Enforcement Wants to Unlock*, by NPR Weekend Edition, originally aired on February 21, 2016, available at http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock. The transcript was printed on February 23, 2016.

24. Attached hereto as **Exhibit V** is a true and correct copy of the document, *Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference*, published by the White House, Office of the Press Secretary, on January 16, 2015, available at https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-. The document was printed on February 23, 2016.

25. Attached hereto as **Exhibit W** is a true and correct copy of the ReCode.com article, *White House. Red Chair. Obama Meets Swisher*, by Kara Swisher, originally published on February 15, 2015, available at http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/. The article was printed on February 23, 2016.

26. Attached hereto as **Exhibit X** is a true and correct copy of the Apple Inc. document, *iCloud: Back up your iOS device to iCloud*, last modified February 11, 2016, available at https://support.apple.com/kb/PH12520. The document was printed on February 23, 2016.

27. Attached hereto as **Exhibit Y** is a true and correct copy of the *Statement to Address Misleading Reports that the County of San Bernardino Reset Terror Suspect's iPhone Without Consent of the FBI*, issued by the Federal Bureau of Investigation to Ars Technhica on February 21, 2016, available at https://assets.documentcloud.org/documents/2716811/Statement-from-the-FBI-Feb-20-2016.pdf. The statement was printed on February 23, 2016.

28. Attached hereto as **Exhibit Z** is a true and correct copy of the New York Times article, *No Smartphone Lies Beyond the Reach of a Judicial Search Warrant*, by Cyrus R. Vance, Jr., originally published on February 18, 2016, available at http://www.nytimes.com/roomfordebate/2016/02/18/crimes-iphones-and-encryption/no-smartphone-lies-beyond-the-reach-of-a-judicial-search-warrant. The article was printed on February 23, 2016.

29. Attached hereto as **Exhibit AA** is a true and correct copy of the Apple Inc. document, *Privacy, Government Information Requests*, available at http://www.apple.com/privacy/government-information-requests/. The document was printed on February 23, 2016.

30. Attached hereto as **Exhibit BB** is a true and correct copy of the BuzzFeed News article, *FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone*, by John Paczkowski and Chris Geidner, last updated on February 20, 2016 available at http://www.buzzfeed.com/johnpaczkowski/apple-terrorists-appleid-passcode-changed-in-government-cust#.pwX6NKVvW. The article was printed on February 23, 2016.

31. Attached hereto as **Exhibit CC** is a true and correct copy of the Washington Post article, *FBI Asked San Bernardino to Reset the Password for Shooter's Phone Backup*, by Ellen Nakashima and Mark Berman, originally published on February 20, 2016, available at https://www.washingtonpost.com/world/ national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-

backup/2016/02/ 20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html. The article was printed on February 23, 2016.

32. Attached hereto as **Exhibit DD** is a true and correct copy of the transcript of the hearing held before the Honorable James Orenstein on October 26, 2015 in *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. 19.

I declare under penalty of perjury of the laws of the United States that the foregoing is true and correct. Executed at Irvine, California on February 25, 2016.

Nicola T. Hanna e/n

Nicola T. Hanna

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

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

MARC J. ZWILLINGER*
marc@zwillgen.com
JEFFFREY G. LANDIS*
jeff@zwillgen.com
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.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

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

ED No. CM 16-10 (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

<u>Hearing</u>:
Date: March 22, 2016
Time: 1:00 p.m.
Place: Courtroom 3 or 4

I, Erik Neuenschwander, declare:

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

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

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

Background

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

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

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

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

Overview of Security of Apple's Devices

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

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

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

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

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

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

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

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

The Government's Request

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

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

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

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

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

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

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

Creating and Testing the Operating System

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

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

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

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

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

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

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

27. After GovtOS is designed and implemented, it will need to be compiled and an installable image will need to be created for the type of device in question. Lastly, it will have to be signed with Apple's cryptographic key verifying that it is Apple-authorized software. Absent Apple's proper cryptographic signature, this device will not load GovtOS.

28. Apple would not agree to sign GovtOS voluntarily because it is not software that Apple wants created, deployed or released.

29. This entire development process would likely be logged and recorded in case Apple's methodology is ever questioned, for example in court.

Quality Assurance and Security Testing

30. Once the operating system is created it will need to go through Apple's quality assurance and security testing process.

31. The quality assurance and security testing process is an integral part of the development and deployment of any hardware or software product Apple creates. Apple's ecosystem is incredibly complicated. Changing one feature of an operating system often has ancillary or unanticipated consequences. The potential for such consequences increases with the number of changes to the operating system. Thus, quality assurance and security testing requires that the new operating system be tested and validated before being deployed. The quality assurance and security testing process requires that Apple test GovtOS internally on multiple devices with the exact same hardware features and operating system as the device at issue, in order to ensure that GovtOS functions as required by the government's request.

32. Here, quality assurance and security testing will be particularly critical because the FBI-commissioned operating system will need to access the data partition of the device in order to test the passcodes. The data partition is where any user data resides. Because the device at issue contains unique data—any damage or modification to which could be irreversible—Apple will have to undertake additional testing efforts to confirm and validate that running this newly developed operating

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

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

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

Deploying the Operating System on the Subject Device

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

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

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

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

Destroying or Securing the Operating System

39. The government's papers suggest that once deployment of GovtOS is completed and the government (presumably) accesses the device, Apple can simply "destroy" GovtOS.

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

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

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

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

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

Burden of Repeated Requests

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

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

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

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

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

Novelty of the Government's Request

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

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

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

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

Alternative Ways of Obtaining Information from the Device

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

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

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

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

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

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

60. Apple iCloud backs up information—including device settings, app data, photos, videos, and conversations in the Messages app—daily over Wi-Fi. In order for an iCloud backup to occur, however, the backup feature must be enabled, and the device must be locked, connected to a power source, signed into iCloud, and have Wi-Fi access to the Internet.

61. Shortly after the shooting, in the course of voluntarily providing the FBI with guidance, Apple recommended to the FBI that that the device be connected to a known Wi-Fi network, such as one at the subject's home or at the SBCPHD, and plugged into a power source so it could potentially create a new iCloud backup automatically. If successful, that backup might have contained information between the last backup and the date of the shooting.

Process of Writing Code

62. I have been writing computer code for thirty years.

63. I started out writing IBM Advanced BASIC.

64. In my experience, different people approach writing code in different ways. Some people write a complete design before starting to code. Others start with the code and write it from start to finish. Still others begin with a sketch of what they want to make, which can be a list of features or an actual physical picture.

65. Writing code is an exceedingly creative and expressive process, requiring a choice of language (*e.g.*, C, C++, Objective-C, Swift, Javascript, Python, Perl, PHP, etc.), a choice of audience (both in terms of the targeted technology platforms and types of end users), a choice of syntax and vocabulary (*e.g.*, variable names, function names, class definitions, etc.), the creation of complex data structures, algorithms to manipulate and transform data, detailed textual descriptions to help explain what the code is doing (*i.e.*, what are called "comments" to code), methods of communicating information to the user (*e.g.*, through words, icons, pictures, sounds, etc.) and receiving and responding to user input—all expressed through human-readable, expressive (and functional) written work product.

66. There are a number of ways to write code to accomplish a given task, some more efficient and more elegant, than others. Moreover, writing software is an iterative, revision intensive, and mentally challenging task, just like writing essays, whitepapers, memos, and even poems.

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

Executed this 25th day of February 2016 in Redwood City, California.

By:________________________
Erik Neuenschwander
Manager of User Privacy
Apple Inc.

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

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

MARC J. ZWILLINGER*
marc@zwillgen.com
JEFFFREY G. LANDIS*
jeff@zwillgen.com
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.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

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

ED No. CM 16-10 (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

I, Lisa Olle, declare:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

By: Lisa Olle
Lisa Olle
Manager, Global Privacy & Law
Enforcement Compliance Team

Apple Inc.