

1 EILEEN M. DECKER  
United States Attorney  
2 PATRICIA A. DONAHUE  
Assistant United States Attorney  
3 Chief, National Security Division  
TRACY L. WILKISON (California Bar No. 184948)  
4 Chief, Cyber and Intellectual Property Crimes Section  
Assistant United States Attorney  
5 1500 United States Courthouse  
312 North Spring Street  
6 Los Angeles, California 90012  
Telephone: (213) 894-2400  
7 Facsimile: (213) 894-8601  
Email: Tracy.Wilkison@usdoj.gov

8 Attorneys for Applicant  
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT  
11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH  
OF AN APPLE IPHONE SEIZED  
13 DURING THE EXECUTION OF A  
SEARCH WARRANT ON A BLACK  
14 LEXUS IS300, CALIFORNIA  
LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)

GOVERNMENT'S REPLY IN SUPPORT  
OF MOTION TO COMPEL AND  
OPPOSITION TO APPLE INC.'S  
MOTION TO VACATE ORDER

DECLARATIONS OF STACEY PERINO,  
CHRISTOPHER PLUHAR, AND TRACY  
WILKISON, AND EXHIBITS FILED  
CONCURRENTLY

Hearing Date: March 22, 2016  
Hearing Time: 1:00 p.m.  
Location: Courtroom of the  
Hon. Sheri Pym

21  
22 Applicant United States of America, by and through its counsel of record, the  
23 United States Attorney for the Central District of California, hereby files its Reply in  
24 Support of the Government's Motion to Compel and Opposition to Apple Inc.'s Motion  
25 to Vacate this Court's February 16, 2016 Order Compelling Apple To Assist Agents In  
26 Its Search.

27 This Reply and Opposition is based upon the attached memorandum of points and  
28 authorities, the concurrently filed declarations of Federal Bureau of Investigation

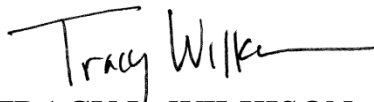
1 (“FBI”) Technical Director of the Cryptologic and Electronic Analysis Unit Stacey  
2 Perino, FBI Supervisory Special Agent Christopher Pluhar, and Assistant United States  
3 Attorney Tracy Wilkison, with attached exhibits, the files and records in this case, and  
4 such further evidence and argument as this Court may permit.  
5

6 Dated: March 10, 2016

Respectfully submitted,

7 EILEEN M. DECKER  
United States Attorney

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

10  
11 

12 TRACY L. WILKISON  
Assistant United States Attorney

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

## **TABLE OF CONTENTS**

<b><u>DESCRIPTION</u></b>	<b><u>PAGE</u></b>
TABLE OF AUTHORITIES .....	ii
I. INTRODUCTION .....	1
II. ARGUMENT.....	3
A. The All Writs Act Is an Integral Part of Our Justice System.....	3
B. Through the All Writs Act, Congress Has Empowered the Court to Decide the Fact-Specific Matter Before It .....	6
1. This Case Must Be Decided on Its Facts .....	6
2. Congressional Inaction Does Not Preclude an AWA Order .....	8
3. CALEA Does Not Forbid the Order .....	10
C. The Order Is Proper Under New York Telephone and the AWA.....	12
1. Apple Is Closely Connected to the Underlying Controversy .....	13
2. The Burden Placed on Apple Is Not Undue and Unreasonable .....	17
a. Writing Code Is Not a Per Se Undue Burden.....	18
b. Apple’s Proffered Estimate of Employee Time Does Not Establish an Undue Burden .....	21
c. Impinging on Apple’s Marketing of Its Products as Search-Warrant-Proof Is Not an Undue Burden .....	22
d. Apple’s Speculation that Third Parties Could Be Harmed in the Future if It Complies With the Order Does Not Establish an Undue Burden on Apple .....	23
e. Cumulative Future Compliance Costs Should Not Be Considered and Are, In Any Event, Compensable.....	27
3. Apple’s Assistance Is Necessary .....	28
D. The Order Does Not Implicate, Let Alone Violate, the First and Fifth Amendments.....	31
1. Incidentally Requiring a Corporation to Add Functional Source Code to a Commercial Product Does Not Violate the First Amendment.....	31
2. There Is No Due Process Right Not to Develop Source Code .....	34
III. CONCLUSION.....	35

## **TABLE OF AUTHORITIES**

<b><u>DESCRIPTION</u></b>	<b><u>PAGE</u></b>
<b>Cases</b>	
<i>Am. Council on Educ. v. F.C.C.</i> ,	
451 F.3d 226 (D.C. Cir. 2006).....	11
<i>Application of United States</i> ,	
610 F.2d 1148 (3d Cir. 1979) .....	19
<i>Baker v. Carr</i> ,	
369 U.S. 186 (1962).....	8
<i>Bank of U.S. v. Halstead</i> ,	
23 U.S. (10 Wheat.) 51 (1825) .....	3, 8, 9, 10
<i>Bankers Life &amp; Casualty Co v. Holland</i> ,	
346 U.S. 379 (1953).....	10
<i>Blair v. United States</i> ,	
250 U.S. 279 (1919).....	28
<i>Branzburg v. Hayes</i> ,	
408 U.S. 665 (1972).....	34
<i>Carrington v. United States</i> ,	
503 F.3d 888 (9th Cir. 2007) .....	10
<i>Cheney v. U.S. Dist. Court</i> ,	
542 U.S. 367 (2004).....	13
<i>Company v. United States</i> ,	
349 F.3d 1132 (9th Cir. 2003) .....	11
<i>County of Sacramento v. Lewis</i> ,	
523 U.S. 833 (1998).....	35
<i>Diamond v. Chakrabarty</i> ,	
447 U.S. 303 (1980).....	7

**TABLE OF AUTHORITIES (CONTINUED)**

<u>DESCRIPTION</u>	<u>PAGE</u>
<i>Envtl. Def. Ctr., Inc. v. U.S. E.P.A.</i> ,	
344 F.3d 832 (9th Cir. 2003) .....	33
<i>F.T.C. v. Dean Foods Co.</i> ,	
384 U.S. 597 (1966).....	9
<i>Full Value Advisors, LLC v. S.E.C.</i> ,	
633 F.3d 1101 (D.C. Cir. 2011).....	33
<i>Gonzalez v. Google</i> ,	
234 F.R.D. 674 (N.D. Cal. 2006) .....	19
<i>Haig v. Agee</i> ,	
453 U.S. 280 (1981).....	19
<i>In re Access to Videotapes</i> ,	
2003 WL 22053105 (D. Md. 2003).....	14
<i>In re Order Authorizing the Use of a Pen Register</i> ,	
538 F.2d 956 (2d Cir. 1976) .....	5
<i>In re Under Seal</i> ,	
749 F.3d 276 (4th Cir. 2014) .....	22
<i>In re XXX Inc.</i> ,	
2014 WL 5510865 (S.D.N.Y. 2014) .....	13
<i>Jacobs v. Clark Cty. Sch. Dist.</i> ,	
526 F.3d 419 (9th Cir. 2008) .....	34
<i>Karn v. United States Department of State</i> ,	
925 F. Supp. 1 (D.D.C. 1996).....	32
<i>Levine v. United States</i> ,	
362 U.S. 610 (1960).....	3
<i>Michigan Bell Tel. Co. v. United States</i> ,	
565 F.2d 385 (6th Cir. 1977) .....	5

**TABLE OF AUTHORITIES (CONTINUED)**

<u>DESCRIPTION</u>	<u>PAGE</u>
<i>Murphy v. Waterfront Comm’n of New York Harbor,</i> 378 U.S. 52 (1964).....	31
<i>Pennsylvania Bureau of Correction v. U.S. Marshals Serv.,</i> 474 U.S. 34 (1985).....	10
<i>Plum Creek Lumber Co. v. Hutton,</i> 608 F.2d 1283 (9th Cir. 1979) .....	20
<i>Price v. Johnston,</i> 334 U.S. 266 (1948).....	4, 10
<i>Railway Mail Assn. v. Corsi,</i> 326 U.S. 88 (1945).....	6, 30
<i>Riley v. California,</i> 134 S. Ct. 2473 (2014).....	1, 7, 31
<i>Rumsfeld v. Forum for Acad. &amp; Institutional Rights, Inc.,</i> 547 U.S. 47 (2006).....	31, 33, 34
<i>Simmons v. United States,</i> 390 U.S. 377 (1968).....	31
<i>In re Application of United States for an Order Authorizing an In-Progress</i> <i>Trace of Wire Commc’ns over Tel. Facilities (Mountain Bell),</i> 616 F.2d 1122 (9th Cir. 1980) .....	passim
<i>U.S. Telecom Ass’n v. F.C.C.,</i> 227 F.3d 450 (D.C. Cir. 2000).....	10
<i>Application of the United States for Relief,</i> 427 F.2d 639 (9th Cir. 1970) .....	11
<i>United States v. Balsys,</i> 524 U.S. 666 (1998).....	32

**TABLE OF AUTHORITIES (CONTINUED)**

<u>DESCRIPTION</u>	<u>PAGE</u>
<i>United States v. Burr</i> ,	
25 F. Cas. 38 (C.C. Va. 1807) .....	20
<i>United States v. Craft</i> ,	
535 U.S. 274 (2002).....	8, 9
<i>United States v. Elcom Ltd.</i> ,	
203 F. Supp. 2d 1111 (N.D. Cal. 2002).....	32
<i>United States v. Fricosu</i> ,	
841 F. Supp. 2d 1232 (D. Colo. 2012) .....	14, 20
<i>United States v. Hall</i> ,	
583 F. Supp. 717 (E.D. Va. 1984) .....	14
<i>United States v. Illinois Bell Tel. Co.</i> ,	
531 F.2d 809 (7th Cir. 1976) .....	5
<i>United States v. Koyomejian</i> ,	
970 F.2d 536 (9th Cir. 1992) .....	11
<i>United States v. New York Telephone Co.</i> ,	
434 U.S. 159 (1977).....	passim
<i>United States v. Nixon</i> ,	
418 U.S. 683 (1974).....	17
<i>United States v. R. Enterprises, Inc.</i> ,	
498 U.S. 292 (1991).....	17
<i>United States v. Sindel</i> ,	
53 F.3d 874 (8th Cir. 1995) .....	33
<i>Univ. of Pennsylvania v. E.E.O.C.</i> ,	
493 U.S. 182 (1990).....	23
<i>Universal City Studios, Inc. v. Corley</i> ,	
273 F.3d 429 (2d Cir. 2001) .....	32

## TABLE OF AUTHORITIES (CONTINUED)

<u>DESCRIPTION</u>	<u>PAGE</u>
<i>Washington v. Glucksberg</i> ,	
521 U.S. 702 (1997).....	35
<i>West Virginia Bd. of Ed. v. Barnette</i> ,	
319 U.S. 624 (1943).....	31
<i>Zivotofsky ex rel. Zivotofsky v. Clinton</i> ,	
132 S. Ct. 1421 (2012).....	7, 8
<i>Zurcher v. Stanford Daily</i> ,	
436 U.S. 547 (1978).....	31
<b>Federal Statutes</b>	
18 U.S.C. §§ 3141-45.....	10
28 U.S.C. § 1291 .....	10
28 U.S.C. § 1651 .....	3
28 U.S.C. §§ 2241-55.....	10
47 U.S.C. § 1002.....	11, 12
47 U.S.C. § 1005.....	12
48 U.S.C. § 1613a.....	10
Pub. L. 80-773, ch. 646, 62 Stat. 944 (June 25, 1948) .....	4
<b>Federal Rules</b>	
Federal Rule of Criminal Procedure 41 .....	5, 8
Federal Rule of Civil Procedure 26 .....	19
<b>Other Authorities</b>	
<i>In the Matter of Commc’ns Assistance for Law Enforcement Act</i>	
& <i>Broadband Access &amp; Servs.</i> , 20 F.C.C. Rcd. 14989 (2005).....	12
H.R. Rep. No. 308, 80th Cong., 1st Sess., A46 (1947) .....	4
Brief for Respondent, <i>United States v. New York Telephone Co.</i> ,	
No. 76-835, 1977 WL 189311 (Apr. 18, 1977).....	23



## **MEMORANDUM OF POINTS AND AUTHORITIES**

### **I. INTRODUCTION**

As Apple Inc. concedes in its Opposition, it is fully capable of complying with the Court's Order. By Apple's own reckoning, the corporation—which grosses hundreds of billions of dollars a year—would need to set aside as few as six of its 100,000 employees for perhaps as little as two weeks. This burden, which is not unreasonable, is the direct result of Apple's deliberate marketing decision to engineer its products so that the government cannot search them, even with a warrant. Thus, the lawful warrant in this case—issued by a neutral magistrate upon a finding of probable cause, pursuant to the procedure blessed by the Supreme Court just two years ago in *Riley v. California*, 134 S. Ct. 2473 (2014)—will be frustrated unless Apple complies with the Order. In passing the All Writs Act, Congress gave courts a means of ensuring that their lawful warrants were not thwarted by third parties like Apple.

The Court's Order is modest. It applies to a single iPhone, and it allows Apple to decide the least burdensome means of complying. As Apple well knows, the Order does not compel it to unlock other iPhones or to give the government a universal “master key” or “back door.” It is a narrow, targeted order that will produce a narrow, targeted piece of software capable of running on just one iPhone, in the security of Apple's corporate headquarters. That iPhone belongs to the County of San Bernardino, which has consented to its being searched. The phone was used by the now-dead terrorist Syed Rizwan Farook, who also consented to its being searched as part of his employment agreement with the County. In short, the Order invades no one's privacy and raises no Fourth Amendment concerns.

The government and the community need to know what is on the terrorist's phone, and the government needs Apple's assistance to find out. For that reason, the Court properly ordered Apple to disable the warrant-proof barriers it designed. Instead of complying, Apple attacked the All Writs Act as archaic, the Court's Order as leading to a “police state,” and the FBI's investigation as shoddy, while extolling itself as the primary

1 guardian of Americans' privacy. (*See* Wilkison Decl. Ex. 1.) Apple's rhetoric is not  
2 only false, but also corrosive of the very institutions that are best able to safeguard our  
3 liberty and our rights: the courts, the Fourth Amendment, longstanding precedent and  
4 venerable laws, and the democratically elected branches of government.

5 Congress intended the All Writs Act to flexibly meet "new problems" like those  
6 devised by Apple. As the Supreme Court held, the Act supplies a basis for a court to  
7 order a third-party corporation to assist in gathering evidence. As the Ninth Circuit held,  
8 that precedent permits a court to order a corporation to program a computer, even if the  
9 corporation objects that doing so will cost it money, divert its technicians, and annoy its  
10 customers. That controlling precedent and the All Writs Act—not Apple's technological  
11 fiat—should determine whether Farook's iPhone will be searched.

12 Apple and its *amici* try to alarm this Court with issues of network security,  
13 encryption, back doors, and privacy, invoking larger debates before Congress and in the  
14 news media. That is a diversion. Apple desperately wants—desperately *needs*—this  
15 case not to be "about one isolated iPhone." But there is probable cause to believe there  
16 is evidence of a terrorist attack on that phone, and our legal system gives this Court the  
17 authority to see that it can be searched pursuant to a lawful warrant. And under the  
18 compelling circumstances here, the Court should exercise that authority, even if Apple  
19 would rather its products be warrant-proof.

20 This case—like the three-factor Supreme Court test on which it must be decided—  
21 is about specific facts, not broad generalities. Here, Apple deliberately raised  
22 technological barriers that now stand between a lawful warrant and an iPhone containing  
23 evidence related to the terrorist mass murder of 14 Americans. Apple alone can remove  
24 those barriers so that the FBI can search the phone, and it can do so without undue  
25 burden. Under those *specific* circumstances, Apple can be compelled to give aid. That  
26 is not lawless tyranny. Rather, it is ordered liberty vindicating the rule of law. This  
27 Court can, and should, stand by the Order. Apple can, and should, comply with it.

## II. ARGUMENT

### A. The All Writs Act Is an Integral Part of Our Justice System

In both its Opposition and its public statements, Apple seeks to characterize the All Writs Act (“AWA” or “Act”), codified at 28 U.S.C. § 1651, as an obscure law dredged up by the government to achieve unprecedented power. That premise is false. The Act is a vital part of our legal system that is regularly invoked in a variety of contexts. Congress intended for the Act to be broad and flexible, capable of rising to meet new obstacles to the courts’ lawful exercise of jurisdiction. The Act is not a judicial usurpation of congressional power, but rather an example of Congress’s reliance upon the courts’ sound discretion and close familiarity with specific facts to ensure that justice is done.

The AWA is indeed venerable. It was enacted by the First Congress at “the very beginning of this Nation” as part of the Judiciary Act of 1789. *See Levine v. United States*, 362 U.S. 610, 615 (1960). The Act codified basic judicial powers critical to justice and the legal system, such as the power to issue writs of habeas corpus and mandamus. Like other foundational laws, it was framed not in a hypertechnical way to address the passing needs of 1789, but in broad, enduring terms that bestowed on the courts the “power to issue . . . all . . . writs . . . which may be necessary for the exercise of their respective jurisdictions, and agreeable to principles and usages of law.”

The Supreme Court quickly recognized that “[t]o limit the operation of [the Act] now, to that which it would have had in the year 1789, would open a door to many and great inconveniencies, which Congress seems to have foreseen, and to have guarded against, by giving ample powers to the Courts, so to mold their process, as to meet whatever changes might take place.” *Bank of U.S. v. Halstead*, 23 U.S. (10 Wheat.) 51, 62 (1825) (interpreting the phrase “agreeable to the usages and principles of law” to be a broad grant of power to the federal courts) (emphasis in original).

In the centuries since, the Act has never fallen into disuse or disrepute. Indeed, few laws are more vital. As the Supreme Court has explained:

1 [T]he writ must be agreeable to the usages and principles of “law,” a term  
 2 which is unlimited by the common law or the English law. And since “law”  
 3 is not a static concept, but expands and develops as new problems arise, we  
 4 do not believe that the forms of [writs] authorized by [the AWA] are only  
 5 those recognized in this country in 1789, when the original Judiciary Act  
 6 containing the substance of this section came into existence. In short, we do  
 7 not read [the AWA] as an ossification of the practice and procedure of more  
 8 than a century and a half ago. Rather it is a legislatively approved source of  
 9 procedural instruments designed to achieve “the rational ends of law.”

10 *Price v. Johnston*, 334 U.S. 266, 282-85 (1948) (discussing the scope of the writ of  
 11 habeas corpus under the AWA), *overruled on other grounds by McCleskey v. Zant*, 499  
 12 U.S. 467 (1991). *Price* further held that because “justice may on occasion require the  
 13 use of a variation or a modification” of the writ, and because Congress had chosen to  
 14 provide broad powers in the AWA, “it follows that we should not write in limitations  
 15 which Congress did not see fit to make.” *Id.* Just months after the Supreme Court  
 16 decided *Price*, Congress responded not by chastening the Court or restricting the AWA,  
 17 but by “extend[ing]” it: first, courts could now issue not just “necessary” writs but also  
 18 “appropriate” writs; second, “all” courts, not just certain enumerated ones, would be  
 19 empowered by the Act. *See* 80 Pub. L. 80-773, ch. 646, 62 Stat. 944 (June 25, 1948);  
 20 H.R. Rep. No. 308, 80th Cong., 1st Sess., A46 (1947) (noting the “revised section  
 21 extends the power to issue writs in aid of jurisdiction”).

22 Apple portrays the AWA as dusty and forgotten so that application of the Act here  
 23 might seem an unprecedented and congressionally unforeseen assumption of judicial  
 24 power. This mischaracterization of the Act was rejected by the Supreme Court in *United*  
 25 *States v. New York Telephone Co.*, 434 U.S. 159 (1977), which held that the AWA is  
 26 properly used to compel a telecommunications company to supply personnel and  
 27 equipment to support a government investigation by installing a pen register. The  
 28 Court’s conclusion was expressly based on *Price*’s holding that the AWA must be  
 “fluid” and evolving, *id.* at 173, thus foreclosing Apple’s current effort to confine *New*  
*York Telephone* to only pen registers.

1 In deciding *New York Telephone*, the Supreme Court directly confronted and  
2 expressly rejected the policy arguments Apple raises now. Like Apple, the telephone  
3 company argued: that Congress had not given courts the power to issue such an order in  
4 its prior legislation; that the AWA could not be read so broadly; that it was for Congress  
5 to decide whether to provide such authority; and that relying on the AWA was a  
6 dangerous step down a slippery slope ending in arbitrary police powers. *See In re Order*  
7 *Authorizing the Use of a Pen Register*, 538 F.2d 956, 962-63 (2d Cir. 1976) (reversed);  
8 *New York Telephone*, 434 U.S. at 179 (Stevens, J., dissenting). The Court dismissed  
9 these arguments in light of *Price*. *See New York Telephone*, 434 U.S. at 173-75 & n.23  
10 (maj. op.). In the forty years since that decision, it has become clear that the Court was  
11 correct because those fears have proved unfounded.

12 The Supreme Court's approach to the AWA does not create an unlimited source of  
13 judicial power, as Apple contends. The Act is self-limiting because it can only be  
14 invoked in aid of a court's jurisdiction. Here, that jurisdiction rests on a lawful warrant,  
15 issued by a neutral magistrate pursuant to Rule 41. And *New York Telephone* provides a  
16 further safeguard, not through bright-line rules but rather through three factors courts  
17 must consider before exercising their discretion: (1) how far removed a party is from the  
18 investigative need; (2) how unreasonable a burden would be placed on that party; and (3)  
19 how necessary the party's assistance is to the government. This three-factor analysis  
20 respects Congress's mandate that the Act be flexible and adaptable, while eliminating the  
21 concern that random citizens will be forcibly deputized.

22 Technology is constantly advancing, but these advances have never required the  
23 AWA to retreat. To the contrary, as the Supreme Court made clear in *Halstead* and  
24 *Price*, the Act must grow and develop to keep pace with "whatever changes might take  
25 place." Courts used that "common sense" in applying the Act to programming and  
26 electronic data in the trap-and-trace context. *See Michigan Bell Tel. Co. v. United States*,  
27 565 F.2d 385, 389 (6th Cir. 1977); *United States v. Illinois Bell Tel. Co.*, 531 F.2d 809,  
28

1 813 (7th Cir. 1976). And this Court applied the same common sense in issuing the  
 2 Order. The AWA is a proper source of this Court’s authority.

3 **B. Through the All Writs Act, Congress Has Empowered the Court to**  
 4 **Decide the Fact-Specific Matter Before It**

5 *1. This Case Must Be Decided on Its Facts*

6 The Order applies to a single device and is based on the specific facts before this  
 7 Court. Those compelling facts justify ordering Apple to remove the barriers to executing  
 8 a warrant for an iPhone used by a terrorist who carried out a mass murder. Apple  
 9 demands that the Court should instead address the broad questions whether Apple should  
 10 be required to unlock *every* iPhone in *every* instance, or whether Apple should be  
 11 required to give the government the means to do so. Those questions are not before this  
 12 Court. Indeed, if Apple’s compliance with the AWA in a single case were sufficient to  
 13 require it to comply in all cases, there would be no dispute here: Apple routinely  
 14 complied with AWA orders in the past. (*See infra* p. 27.) In the same respect, future  
 15 cases involving other iPhones will be decided on *their* specific facts.

16 The “case or controversy” before the Court is narrow and specific, as well it  
 17 should be. “[T]he very strength of our common law” is “its cautious advance and retreat  
 18 a few steps at a time.” Benjamin Cardozo, *The Growth of the Law* 6 (1924). It is  
 19 precisely the rich facts of a particular case that provide the basis for a court to resolve it,  
 20 and these same facts ensure that the law’s growth is incremental and thoughtful. That is  
 21 why courts resolve cases and controversies that are “definite and concrete, not  
 22 hypothetical or abstract.” *Railway Mail Assn. v. Corsi*, 326 U.S. 88, 93 (1945).

23 Only by stripping this case of its “definite and concrete” facts—the very facts that  
 24 guide the AWA inquiry—and by recasting the case as a “hypothetical or abstract” policy  
 25 debate can Apple invoke separation of powers and the political-question doctrine. (Opp.  
 26 18-19.) Apple urges the Court to focus on broader policy issues, and then proclaims that  
 27 the Court is forbidden to resolve them. But the actual issue before this Court—whether  
 28 Apple can be directed under the AWA to provide specific technical assistance—is not a



1 judicially imponderable question forbidden by separation of powers: courts resolve such  
2 questions regularly, as in *New York Telephone* and *In re Application of United States for*  
3 *an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*  
4 (*"Mountain Bell"*), 616 F.2d 1122, 1126-29 (9th Cir. 1980). Nor must courts flee from  
5 cases involving policy and privacy considerations related to searching smartphones.  
6 Less than two years ago, the Supreme Court confronted just such issues in *Riley v.*  
7 *California*. The Court, after carefully considering smartphones' technology and their  
8 role in society, held that an "appropriate balance" between privacy concerns and  
9 investigative needs was struck by the government's obtaining a search warrant. 134 S.  
10 Ct. at 2484. The Court added that its "holding, of course, is not that the information on a  
11 cell phone is immune from search; it is instead that a warrant is generally required before  
12 such a search." *Id.* at 2493. Thus, Apple's privacy questions, far from being  
13 unanswerable by any court, have already *been* answered by the Supreme Court, and the  
14 government complied with *Riley* by obtaining a warrant here.

15 This case also does not present a "political question," as suggested by Apple. The  
16 ongoing debate regarding law enforcement, national security needs, and privacy does not  
17 deprive this Court of authority to issue the Order. In fact, Apple's argument is undone  
18 by the very authority it cites: *Diamond v. Chakrabarty*, 447 U.S. 303 (1980). (Opp. 19.)  
19 Far from refusing to decide a case because of the policy implications before it, the  
20 Supreme Court explained that the "grave risks" and "parade of horrors" conjured up by  
21 the petitioner and his *amici* needed to be presented to Congress, while the Court would  
22 decide the case instead by applying the broad terms Congress used in 1930 Patent Act.  
23 *Id.* at 316-18. As *Diamond* shows, the political-question doctrine is a "narrow  
24 exception" to the general rule that "the Judiciary has a responsibility to decide cases  
25 properly before it." *Zivotofsky ex rel. Zivotofsky v. Clinton*, 132 S. Ct. 1421, 1427  
26 (2012). It applies not in every case raising policy considerations but only in cases that  
27 raise nothing *but* policy considerations, cases where there is "a lack of judicially  
28

discoverable and manageable standards for resolving” the issue.<sup>1</sup> *Baker v. Carr*, 369 U.S. 186, 217 (1962). Here, as in *Diamond*, the AWA standards already have been “judicially discover[ed]” and have proven “manageable” for decades—indeed, for centuries. The advent of iOS 9 does not alter the authority of the AWA or require this Court to abstain, nor do public and political interest in this case.

## 2. *Congressional Inaction Does Not Preclude an AWA Order*

As the Supreme Court has made clear, Congress’s broad grant of judicial authority under the AWA was designed to avoid the need for more specific, piecemeal legislation. A lack of more specific legislation is thus no barrier to the Order. Apple insists that this Court lost its power under the AWA because the executive branch chose not to propose amendments to CALEA, and because Congress might someday pass other legislation. (Opp. 8-10.) But the Supreme Court has repeatedly made clear “that failed legislative proposals are a particularly dangerous ground on which to rest an interpretation of a prior statute, reasoning that congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction, including the inference that the existing legislation already incorporated the offered change.” *United States v. Craft*, 535 U.S. 274, 287 (2002).

Until very recently, there was widespread agreement that the AWA sufficed in this area. As Apple itself has acknowledged, “it seemed that this had been somewhat settled views and settled authority from multiple judges.” (Hanna Decl. Ex. DD at 56.) Indeed, Apple has conceded that the recent decision of a Magistrate Judge in the Eastern District of New York “mark[ed] the first time a judge has questioned the authority of the All Writs Act to grant supplemental orders to accompany . . . warrants” to search iPhones.

---

<sup>1</sup> A case can also be irresolvable in the rare event that “there is a textually demonstrable constitutional commitment of the issue to a coordinate political department.” *Zivotofsky*, 132 S. Ct. at 1427. But no such commitment exists here. The issuance of writs is a traditional part of the courts’ authority. *See Halstead*, 23 U.S. at 61-62. The AWA exists to further a court’s jurisdiction. Congress has indisputably given this Court jurisdiction to issue search warrants through Rule 41(b), and power to issue writs in furtherance of those warrants through the AWA.



(Wilkison Decl. Ex. 16 at 3; *see* Exhibit A to Apple’s Notice of Supplemental Authority (“New York Order”).) Thus, there is—at a minimum—an “equally tenable inferenc[e]” that “existing legislation already incorporated” the power to order Apple to assist in executing search warrants. *Craft*, 535 U.S. at 287. That inference is all the more powerful because there was never even a “failed legislative proposal” of a “CALEA II” bill (Opp. 9), merely vague discussions about potential legislation that would have placed broader obligations, not at issue here, on some communications service providers.

The Supreme Court has emphasized the prohibition on drawing meaning from congressional silence in the AWA context. In *F.T.C. v. Dean Foods Co.*, 384 U.S. 597, 600 (1966), a circuit court dissolved an FTC restraining order on the ground that, in two different Congresses, “bills sponsored by the said Commission were introduced, which bills if enacted into law would have conferred upon the Commission such authority as it is attempting to exercise in the case now before this court.” The Supreme Court reversed, reaffirming two key principles: (1) congressional inaction, past or future, is uninformative; and (2) because the AWA creates power *absent* congressional legislation, there is no need for Congress to specifically confer it. “Congress neither enacted nor rejected these proposals; it simply did not act on them. Even if it had, the legislation as proposed would have had no affect whatever on the power that Congress granted the courts by the All Writs Act. We cannot infer from the fact that Congress took no action at all . . . an intent to circumscribe traditional judicial remedies.” *Id.* at 609. That holding was echoed in *New York Telephone*, which made clear that the AWA empowers a court to act “unless appropriately confined by Congress.” 434 U.S. at 172-73.<sup>2</sup>

---

<sup>2</sup> In a recent and first-of-its-kind ruling, the New York Order—without addressing *Dean Foods*—held that interpreting the AWA to empower courts absent specific congressional authorization would violate separation-of-powers principles by bestowing legislative functions on the courts. (New York Order 21-30.) The government has sought review from the district court overseeing that matter, and the order has no precedential value here. Moreover, its reasoning suffers from fatal flaws. First, this argument was expressly rejected in *Halstead*, 23 U.S. at 61-62 (stating that Congress’s check on abusive writs by federal courts is for it to “correct the evil by more specific legislation” rather than having Congress specifically authorize each exercise of the court’s authority), and was raised by the dissent in *New York Telephone*, in 434 U.S. at (footnote cont’d on next page)

1 In short, the AWA does not require any *additional* legislation to empower the  
 2 courts. Rather, as *Dean Foods* and *New York Telephone* held, the courts retain the  
 3 flexible power bestowed by Congress through the AWA unless Congress expressly takes  
 4 it away. As explained below, Congress has not enacted legislation that specifically  
 5 confines the courts' power here. Its silence says nothing.

### 6 3. CALEA Does Not Forbid the Order

7 Contrary to Apple's claims (Opp. 16-19), CALEA did not deprive this Court of its  
 8 power to issue the Order. Congress's intent in passing CALEA was not to weaken  
 9 existing judicial powers under the AWA, but to "preserve the status quo" regarding the  
 10 lawful interception of transmissions. *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 455  
 11 (D.C. Cir. 2000). The statute does not address the particular issue before this Court.

12 As explained above, the AWA "is controlling" unless "a statute *specifically*  
 13 addresses the *particular* issue at hand." *Pennsylvania Bureau of Correction v. U.S.*  
 14 *Marshals Serv.*, 474 U.S. 34, 43 (1985) (emphases added). Put otherwise, it is not

---

15  
 16 179 & n.1 (arguing, for example, that, in light of the limits of Title III, any application of  
 17 the AWA to pen registers "must await congressional deliberation"), and rejected by the  
 18 majority, *id.* at 175 n.23 (maj. op.).

19 Second, the AWA codified the courts' pre-existing, common-law power to issue  
 20 writs to enforce the courts' jurisdiction. Thus, the idea that judges would continue to  
 21 determine the scope of these writs would neither surprise nor frighten the Framers. *See*  
 22 *also Price*, 334 U.S. at 282-85. That power is not "legislative" in a historical or modern  
 23 sense. *See Halstead*, 23 U.S. at 61-62 ("It is said, however, that this is the exercise of  
 24 legislative power, which could not be delegated by Congress to the Courts of justice.  
 25 But this objection cannot be sustained.").

26 Third, the New York Order is too narrowly focused on the AWA in the context of  
 27 evidence gathering. The AWA also codifies, for example, the writs of mandamus and  
 28 coram nobis. In both of these areas (appellate jurisdiction and post-conviction relief),  
 there is *extensive* congressional legislation setting forth clear limits on the courts' power,  
 defining not only what they may do but also when they may do it. Regarding appellate  
 jurisdiction, Congress has enacted, at a minimum, 28 U.S.C. §§ 1291, 1292, 1295, 2255;  
 18 U.S.C. §§ 3141-45, 3731, 3742; and 48 U.S.C. § 1613a. Nevertheless, pursuant to the  
 AWA, the courts maintain the power to hear any appeal, at any time, provided there is a  
 "clear abuse of discretion" by the district court. *Bankers Life & Casualty Co v. Holland*,  
 346 U.S. 379 (1953). Similarly, Congress has aggressively legislated in the area of post-  
 conviction relief, first in the Judiciary Act of 1948 and then in the Anti-Terrorism and  
 Effective Death Penalty Act. *See* 28 U.S.C. §§ 2241-55. And yet, pursuant to the AWA,  
 the courts maintain the power to grant relief through the writ of coram nobis. *See*  
*Carrington v. United States*, 503 F.3d 888, 890 (9th Cir. 2007), *opinion amended on*  
*denial of reh'g*, 530 F.3d 1183 (9th Cir. 2008).

1 enough for other laws to brush up against similar issues. Rather, Congress must legislate  
 2 so “intricately” as to leave “no gap to fill.” *The Company v. United States*, 349 F.3d  
 3 1132, 1145 n.26 (9th Cir. 2003). A rare instance of a court finding such pervasive  
 4 legislation is *Application of the United States for Relief*, 427 F.2d 639 (9th Cir. 1970), in  
 5 which the Ninth Circuit held that Title III occupied the field of intercepted wire  
 6 communications and precluded use of the AWA to compel a telephone company’s  
 7 assistance. But both Congress and the Supreme Court concluded that the Ninth Circuit’s  
 8 decision was wrong. *See New York Telephone*, 434 U.S. at 178 n.25. Moreover, the  
 9 Supreme Court held that Title III had no effect on the exercise of the AWA in the  
 10 adjacent area of pen registers, *id.* at 166, rejecting the dissent’s arguments to the  
 11 contrary, *id.* at 179 n.1 (Stevens, J., dissenting).

12 CALEA, passed in 1994, does not “meticulously,” “intricately,” or “specifically”  
 13 address when a court may order a smartphone manufacturer to remove barriers to  
 14 accessing stored data on a particular smartphone. Rather, it governs what steps  
 15 telecommunications carriers involved in transmission and switching must take *in*  
 16 *advance* of court orders to ensure their systems can isolate information to allow for the  
 17 real-time interception of network communications. 47 U.S.C. § 1002(a)(1)-(4); *see Am.*  
 18 *Council on Educ. v. F.C.C.*, 451 F.3d 226, 227-28 (D.C. Cir. 2006). As the Ninth Circuit  
 19 has recognized, regulation in a distinct area of law should not “curtail the government’s  
 20 powers in domestic law enforcement” under the AWA. *United States v. Koyomejian*,  
 21 970 F.2d 536, 542 (9th Cir. 1992) (en banc). CALEA thus does not confine the Court’s  
 22 power under the AWA here.

23 Apple points to a section in CALEA stating that “this subchapter does not  
 24 authorize any law enforcement agency . . . to require any specific design of equipment,  
 25 facilities, services, features, or system configurations to be adopted by any provider of a  
 26 wire or electronic communication service, any manufacturer of telecommunications  
 27 equipment, or any provider of telecommunications support services.” (Opp. 16); 47  
 28 U.S.C. § 1002(b)(1)(A), (B). Congress’s wording here is clear and deliberate. The

provision does not destroy any existing authority—or even speak to courts’ power at all. Nor does the provision have any effect outside of CALEA itself: it limits only the authority given to “law enforcement agenc[ies]” by “this subchapter.” The purpose of the provision is not to impliedly deprive the courts of power under the AWA, but to clarify that the preceding subsection of CALEA, 47 U.S.C. § 1002(a), does not permit law enforcement to dictate the “specific design” of the listed items.

To apply that limitation to the Court’s Order would defy both the statutory language and Supreme Court precedent for four reasons: (1) the Order rests not on CALEA, but on the AWA; (2) the Order is an exercise of judicial, not agency authority; (3) the Order does not dictate “any specific design”; and (4) the Order is not directed at an item or service provider listed in § 1002(b)(1)(A), (B).<sup>3</sup> Accordingly, this limitation within CALEA does not restrict the Court’s authority under the AWA, let alone dictate the result in this case.

### **C. The Order Is Proper Under *New York Telephone* and the AWA**

This Court had authority to issue the Order pursuant to the AWA, and Apple has demonstrated no discretionary reason to withdraw it. As Apple recognizes, this Court must consider three equitable factors: (1) how “far removed” Apple is “from the underlying controversy”; (2) how “unreasonable [a] burden” the Order would place on Apple; and (3) how “necessary” its assistance is to searching Farook’s iPhone.<sup>4</sup> *See New*

<sup>3</sup> With regard to the development and control of iOS, Apple is not a provider of wire or electronic communication services but a software developer and licensor. While Apple may be a provider of electronic communication services in its capacity as provider of FaceTime and iMessage, the Court’s order does not bear at all upon the operation of those programs on Farook’s iPhone, let alone generally. *See In the Matter of Commc’ns Assistance for Law Enforcement Act & Broadband Access & Servs.* 20 F.C.C. Rcd. 14989, at ¶ 21 (2005) (recognizing that an entity could provide multiple kinds of services, and holding that the CALEA analysis must be performed on individual components, not the entity as a whole). Nor is Apple an “equipment manufacturer” as that term is used in CALEA. In CALEA, that term refers to a “manufacturer[] of [] telecommunications transmissions and switching equipment,” *see* 47 U.S.C. § 1005—carrier-level equipment, not end-user phones.

<sup>4</sup> The New York Order wrongly posited that there were actually *two* three-part tests: the *New York Telephone* test discussed here, and a statutory one based on the AWA’s text. The New York Order cited in support of its statutory test only cases which  
(footnote cont’d on next page)

1 *York Telephone*, 434 U.S. at 172-75. This test appropriately guides a court’s discretion  
 2 to ensure that the Act does not lead down the slippery slope Apple and *amici* imagine.  
 3 Here, the factors support the Court’s Order.

4 *1. Apple Is Closely Connected to the Underlying Controversy*

5 Apple is not so far removed from the underlying controversy that it should be  
 6 excused from assisting in the execution of the search warrant. In *New York Telephone*,  
 7 the phone company was sufficiently close to the controversy because the criminals used  
 8 its phone lines. *See* 434 U.S. at 174. The Court did not require that the phone company  
 9 know criminals were using its phone lines, or that it be involved in the crime. *See id.*  
 10 Here, as a neutral magistrate found, there is probable cause to believe that Farook’s  
 11 iPhone contains evidence related to his crimes. That alone would be sufficient proximity  
 12 under the AWA and *New York Telephone*, even if Apple did not also own and control the  
 13 software on Farook’s iPhone.

14 Apple attempts to distinguish itself from *New York Telephone* and companies that  
 15 have been compelled to provide technical assistance by claiming that (1) it is “unlike a  
 16 telecommunications monopoly” and (2) it has “merely . . . placed a good into the stream  
 17 of commerce,” as if Apple surrenders control over its iPhones upon selling them. (Opp.  
 18 21.) These distinctions fail on both the facts and the law.

19 To begin with, courts have already issued AWA orders to “manufacturer[s] [such  
 20 as Apple] to attempt to unlock . . . cellphone[s] so that . . . warrant[s] may be executed.”  
 21 *See, e.g., In re XXX Inc.*, 2014 WL 5510865, at \*1-\*3 (S.D.N.Y. 2014); *United States v.*  
 22 *Blake*, No. 13-CR-80054, ECF No. 207 at 5 (S.D. Fl. July 14, 2014). These orders show  
 23 there is no bright-line rule that a third party must be a public utility to fall within the

---

24  
 25 predate *New York Telephone*. (New York Order at 11.) In fact, the *New York Telephone*  
 26 test was meant as a specific application of the general AWA standards, supplanting any  
 27 previous statutory tests. The Supreme Court has articulated a similar context-specific  
 28 three-factor test for the writ of mandamus which supplants any need to create a statutory  
 test. *See Cheney v. U.S. Dist. Court*, 542 U.S. 367, 380-81 (2004). The New York  
 Order’s approach disregards not just *New York Telephone*, but also *Halstead*’s  
 interpretation of “usages and principles of law.”



1 Act's reach. So do other cases. *See, e.g., New York Telephone*, 434 U.S. at 174  
2 (collecting examples of individuals compelled via the AWA); *United States v. Hall*, 583  
3 F. Supp. 717, 722 (E.D. Va. 1984) (credit card company); *In re Access to Videotapes*,  
4 2003 WL 22053105, at \*3 (D. Md. 2003) (landlord); *United States v. Fricosu*, 841 F.  
5 Supp. 2d 1232, 1235 (D. Colo. 2012) (individual). Regardless, Apple's size, technology,  
6 and ubiquity make it akin to the companies in *New York Telephone* and *Mountain Bell*.

7 Moreover, Apple maintains a continued connection to its phones well beyond their  
8 sale, and has deliberately developed its phones so that Apple alone holds the means for  
9 courts' search warrants to be carried out. As Apple's business model and its  
10 representations to its investors and customers make clear, Apple intentionally and for  
11 commercial advantage retains exclusive control over the software that can be used on  
12 iPhones, giving it monopoly-like control over the means of distributing software to the  
13 phones. As detailed below, Apple does so by: (1) firmly controlling iPhones' operating  
14 systems and first-party software; (2) carefully managing and vetting third-party software  
15 before authenticating it for use on iPhones; and (3) continually receiving information  
16 from devices running its licensed software and its proprietary services, and retaining  
17 continued access to data from those devices about how its customers are using them.  
18 Having established suzerainty over its users' phones—and control over the precise  
19 features of the phones necessary for unlocking them—Apple cannot now pretend to be a  
20 bystander, watching this investigation from afar.

21 First, Apple develops its own operating system, and “is *unique* in that it designs  
22 and develops nearly the *entire solution* for its products, including the hardware,  
23 operating system, numerous software applications and related services.” (Wilkison Decl.  
24 Ex. 2 at 8 (Apple 10-K) (emphases added).) Apple's “business strategy leverages its  
25 unique ability to design and develop its own operating systems, hardware, application  
26 software and services.” (*Id.* at 1.) “The tight integration of hardware and software on  
27 iOS devices ensures that each component of the system is trusted, and validates the  
28

1 system as a whole.” (Hanna Decl. Ex. K at 5 (describing how each step is analyzed and  
2 vetted “[f]rom initial boot-up to iOS software updates to third-party apps”).)

3 Second, and pivotally, Apple’s devices will not run software that is not  
4 electronically “signed” by Apple. (*Id.* at 6 (“only Apple-signed code can be installed on  
5 a device”); Hanna Decl. Ex. DD at 64 (“We agree with the government that the system  
6 requires Apple authentication.”).) Through its exclusive control of its electronic  
7 signature, Apple carefully manages and vets both the software updates and all third-party  
8 programs (“apps”) that can be used on its devices. This keeps Apple close to its phones  
9 long after they are sold. As set forth in its licensing agreement, Apple will—if allowed  
10 by the user—periodically check with its devices to send signed updates, and will  
11 “automatically download and install [them] onto [the] device[s].” (Wilkison Decl. Ex. 3  
12 at ¶ 2(h).) Apple also permits only two kinds of apps to be loaded onto iOS devices  
13 through Apple’s App Store: those “developed . . . by Apple” and those “developed . . .  
14 by a third party developer.” (Wilkison Decl. Ex. 4 at 15.) Apple exercises power over  
15 both, because they must be signed by Apple. (Hanna Decl. Ex. K at 18; *see also* Perino  
16 Decl. Ex. 30 at 1 (“Before your app can integrate app services, be installed on a device,  
17 or be submitted to the App Store, it must be signed with a certificate issued by Apple.”).)

18 Third, Apple maintains a connection with its phones after sale by continuing to  
19 receive information from the devices and continuing to access data about how its  
20 customers are using their phones. Indeed, Apple *requires* its users to consent to Apple’s  
21 continued use of data: “When you use your device, your phone number and certain  
22 unique identifiers for your iOS Device are sent to Apple in order to allow others to reach  
23 you by your phone number when using various communication features of the iOS  
24 Software, such as iMessage and FaceTime. . . . Other iOS Software features may require  
25 information from your iOS Device.” (Wilkison Decl. Ex. 3 at ¶ 4.) Apple similarly  
26 expects its customers to consent to its continual monitoring of information in order to get  
27  
28

1 and use certain apps and services.<sup>5</sup> Apple’s connection to its iPhones is not abstract: at a  
 2 minimum, Apple was communicating with Farook’s iPhone as late as October 2015,  
 3 when it last backed up some of the phone’s data on its iCloud server. (Pluhar Decl. ¶ 8.)

4 Thus, by its own design, Apple remains close to its iPhones through careful  
 5 management and constant vigil over what software is on an iPhone and how that  
 6 software is used. Indeed, Apple is much less “removed from the controversy”—in this  
 7 case, the government’s inability to search Farook’s iPhone—than was the *New York*  
 8 *Telephone* company because that company did not deliberately place its phone lines to  
 9 prevent inconspicuous government access. 434 U.S. at 161-62. Here, Apple has  
 10 deliberately used its control over its software to block law-enforcement requests for  
 11 access to the contents of its devices, and it has advertised that feature to sell its products.  
 12 As Apple put it: “Unlike our competitors, Apple cannot bypass your passcode and  
 13 therefore cannot access this data. So it’s not technically feasible for us to respond to  
 14 government warrants for the extraction of this data from devices in their possession  
 15 running iOS 8.”<sup>6</sup> (Wilkison Decl. Ex. 5 at 2.)

16 In short, Apple is not some distant, disconnected third party unexpectedly and  
 17 arbitrarily dragooned into helping solve a problem for which it bears no responsibility.  
 18 Rather, Apple is intimately close to the barriers on Farook’s locked iPhone because  
 19 Apple specifically designed the iPhone to create those barriers.

---

21  
 22 <sup>5</sup> (See, e.g., Wilkison Decl. Ex. 4 at 5 (providing that on any device, iOS or not,  
 23 that uses iTunes Match, Apple “automatically scans the song files and collects other  
 24 information . . . to identify media in your iTunes library,” and “Apple will log  
 25 information such as the tracks you play, stop or skip, the devices you use, and the time  
 26 and duration of playback”); *id.* at 22 (same for iCloud Music Library); *id.* at 5-6  
 (providing Apple’s Genius service will “automatically collect information . . . such as  
 your play history and playlists”); *id.* at 16 (“When you opt in to Popular Near Me via  
 enabling Location Services, Apple will . . . automatically collect information related to  
 certain of your App Store Products, such as your time spent with each App Store Product  
 and the number of times each App Store Product is launched.”).)

27 <sup>6</sup> Apple later modified this language: “Apple will not perform iOS data extractions  
 28 in response to government search warrants.” (Hanna Decl. Ex. AA at 2.)



1                   2.     *The Burden Placed on Apple Is Not Undue and Unreasonable*

2             In seeking to avoid compliance with this Court’s Order, Apple must show that the  
3 burden placed upon it is undue, unreasonable, and noncompensable. *See Mountain Bell*,  
4 616 F.2d at 1122, 1132 (“Appellants did not show that the trace . . . significantly  
5 increased the possibility of a malfunction . . . . Nor did appellants prove that the  
6 compensation provided for in the Order was in any way inadequate.”); *cf. United States*  
7 *v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) (“Consequently, a grand jury subpoena  
8 issued through normal channels is presumed to be reasonable, and the burden of showing  
9 unreasonableness must be on the recipient who seeks to avoid compliance.”). Apple has  
10 shown none of those things. Neither coding software, nor facing speculative business  
11 concerns, nor providing possible future compliance poses an undue burden for Apple.

12             Apple is one of the richest and most tech-savvy companies in the world, and it is  
13 more than able to comply with the AWA order. Indeed, it concedes it can do so with  
14 relatively little effort. Even this modest burden is largely a result of Apple’s own  
15 decision to design and market a nearly warrant-proof phone. In evaluating whether the  
16 burden on Apple is undue, this Court can and should recognize the fundamental  
17 importance that access to evidence plays in the American system of justice. Given “our  
18 historic commitment to the rule of law” and “our view that the twofold aim (of criminal  
19 justice) is that guilt shall not escape or innocence suffer,” the Supreme Court has  
20 recognized that “[t]he need to develop all relevant facts in the adversary system is both  
21 fundamental and comprehensive.” *United States v. Nixon*, 418 U.S. 683, 708-09  
22 (1974). The Court further explained that “[t]he ends of criminal justice would be  
23 defeated if judgments were to be founded on a partial or speculative presentation of the  
24 facts. The very integrity of the judicial system and public confidence in the system  
25 depend on full disclosure of all the facts.” *Id.* at 709. Apple’s position that it cannot be  
26 required to assist with the execution of a warrant for one of its phones flies in the face of  
27 these principles and this tradition.  
28

1                   a.       *Writing Code Is Not a Per Se Undue Burden*

2       Apple’s primary argument regarding undue burden appears to be that it should not  
3 be required to write any amount of code to assist the government. Apple insists that “no  
4 court has ever held that the AWA permits the government to conscript a private  
5 company to build software for it.” (Opp. 31.) Indeed, Apple proclaims that no company  
6 has ever been asked via the Act to write even “some amount of code to gather  
7 information.” (Opp. 27.) This claim is false. More than 35 years ago, in *Mountain*  
8 *Bell*—a case binding here but unmentioned in the recent New York Order—the Ninth  
9 Circuit confronted and rejected exactly that argument. There, as here, appellant made  
10 “[a] great deal” of the burden of coding, 616 F.2d at 1126, but the Circuit demurred. It  
11 recognized that the AWA order at issue would need to be “accomplished by  
12 *programming* a control computer to ‘trap’ incoming calls to the designated telephone  
13 number. Computers that route the incoming calls from the exchange in which they  
14 originate[d] from the dialing telephone [were] *programmed*. In this case twelve  
15 computers were *programmed*, including those in the Phoenix metropolitan area.” *Id.* at  
16 1127 (emphases added). Further, this additional programming caused the phone  
17 company’s computers to operate much less efficiently. *Id.* Nevertheless, the Circuit  
18 held that the lower court “had the *power* to compel [the corporation] to perform” the  
19 programming because “[t]he principles announced in *New York Telephone* . . . compel  
20 the same result here.” *Id.* at 1128-29 (emphasis added).

21       Like Apple, the corporation protested, arguing “that the technological differences  
22 between pen registers” and trap-and-trace programming “serve to distinguish this case.”  
23 *Id.* at 1129-30. The company also complained that the AWA order made it bear “the  
24 entire responsibility for the search.” *Id.* at 1129. It further insisted that the requirement  
25 to reprogram its computers “(1) resulted in a serious drain upon existing personnel and  
26 equipment; and (2) increased the likelihood of system malfunctions while at the same  
27 time impairing the company’s ability to correct such problems.” *Id.* at 1132. It insisted  
28 that the order would deprive it of “irreplaceable services provided by key personnel and

1 [cause] the loss of use of various important pieces of equipment.” (Wilkison Decl. Ex. 6  
 2 at 24-25.) The Circuit was unpersuaded. “[I]t appears to this court to make little  
 3 difference whether . . . company technicians acting at the behest of federal officials” are  
 4 required to ensure that “a computer is programmed to detect electronic impulses which,  
 5 when decoded [by the software], provide a list of telephone numbers.” *Id.*<sup>7</sup>

6 Moreover, *Mountain Bell* was not even the first case to uphold an AWA order  
 7 compelling computer programming. The Third Circuit did the same in *In Re Application*  
 8 *of the United States*, 610 F.2d 1148, 1154 (3d Cir. 1979). There, as here and in  
 9 *Mountain Bell*, the corporation was ordered to program a computer to help gather data  
 10 for the government. *Id.* at 1152-53.<sup>8</sup> The corporation, like Apple, complained that “the  
 11 technical procedures of tracing require that telephone company personnel, not federal  
 12 officers, fully execute the traces.” *Id.* at 1155. And, foreshadowing Apple’s arguments,  
 13 the company also complained that the work it was being asked to undertake “require[d]  
 14 more extensive and more burdensome involvement on the part of the . . . company” than  
 15 did the pen registers in *New York Telephone*. *Id.* at 1150. The Circuit rejected these  
 16 complaints because, among other things, the corporation’s refusal to help would  
 17 otherwise serve “to frustrate the execution of the courts’ warrants and to obstruct  
 18 criminal investigations.” *Id.* at 1155. Thus, there is nothing novel or *per se* unduly  
 19 burdensome about requiring Apple to write code.

---

21 <sup>7</sup> Similarly, in the context of a motion to compel Google, Inc. to produce records  
 22 pursuant to a civil subpoena, a district court held that “creat[ing] new code to format and  
 23 extract query and URL data from many computer banks, in total requiring up to eight  
 24 full time days of engineering time” was a burden that could be overcome through  
 25 compensation. *Gonzalez v. Google*, 234 F.R.D. 674, 683 (N.D. Cal. 2006). Although  
 26 the undue-burden analysis under Federal Rules of Civil Procedure 26 and 45 differs from  
 the analysis under the AWA, it is instructive that in a civil lawsuit—where importance of  
 evidence gathering is certainly less compelling than in a criminal investigation of a  
 terrorist act—a district court compelled a private company to create code. “It is ‘obvious  
 and unarguable’ that no governmental interest is more compelling than the security of  
 the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981).

27 <sup>8</sup> While the tracing programs required little time to input once developed, as  
 28 likely is the case here, the programs undoubtedly took longer to develop in the first  
 place. *See Application of the United States*, 610 F.2d at 1152.

1 Contrary to Apple’s argument, the Order does not require it to “provide decryption  
2 services” to the government. (Opp. 14.) But that would not be novel, either. Indeed, no  
3 less an authority than Chief Justice Marshall held that Aaron Burr’s clerk could be  
4 forced to decipher a coded letter of Burr’s, provided that doing so would not incriminate  
5 the clerk. *See United States v. Burr*, 25 F. Cas. 38, 39-40 (C.C. Va. 1807). Or, to take a  
6 more recent example, the court in *Fricosu*, 841 F. Supp. 2d at 1235, 1237, held that the  
7 AWA empowered it to demand the decryption of a laptop, provided that the act of  
8 decryption itself would not be used to incriminate the defendant. Here, Apple will not  
9 incriminate itself by removing barriers to the lawful search of Farook’s iPhone.

10 To the extent that Apple seeks to analogize its burden to the one in *Plum Creek*  
11 *Lumber Co. v. Hutton*, 608 F.2d 1283 (9th Cir. 1979), it is mistaken. In *Plum Creek*, the  
12 government sought to compel a company that was the target of an investigation to allow  
13 its employees to wear a large monitoring device while working in its sawmill. *Id.* at  
14 1285-86. In addition to distracting the workers, these devices could get caught in the  
15 mill’s equipment, creating an obvious physical danger to the workers. *Id.* at 1289 & n.4.  
16 As the district court explained, the company bore “all the safety risks and [would] pay[]  
17 the cost of all industrial accidents.” *Id.* at 1286. Weighed against the danger to the  
18 workers was the weaker interest of reducing the time required for the investigation: far  
19 from being necessary, the devices were simply a convenience. *Id.* at 1289 & nn.5, 6.  
20 Under those circumstances, the Court would not extend *New York Telephone*.

21 Simply put, none of the special considerations in *Plum Creek* are present here: the  
22 Order does not put Apple’s employees in immediate physical peril; Apple is not being  
23 required to assist in an investigation into itself; the government has offered to  
24 compensate Apple; and—as explained below—Apple’s assistance is not a luxury in an  
25 OSHA investigation but a necessity in investigating a terrorist attack. *Mountain Bell*,  
26 which postdates *Plum Creek* and relates to a much closer factual scenario, provides  
27 better guidance. And as in *Mountain Bell*, the burden on Apple is not undue.

b. *Apple's Proffered Estimate of Employee Time Does Not Establish an Undue Burden*

Apple asserts that it would take six to ten employees two to four weeks to develop new code in order to carry out the Court's Order. (Opp. 13; Neuenschwander Decl. ¶¶ 22-25.) Even taking Apple at its word, this is not an undue burden, especially given Apple's vast resources and the government's willingness to find reasonable compromises and provide reasonable reimbursement.

Apple is a Fortune 5 corporation with tremendous power and means: it has more than 100,000 full-time-equivalent employees and had an annual income of over \$200 billion dollars in fiscal year 2015—more than the operating budget for California. (*Compare* Wilkison Decl. Ex. 2 at 9, 24, 41 (Apple 10-K), *with* Ex. 7 (FY 2015-16 budget).) Indeed, Apple's revenues exceed the nominal GDPs of two thirds of the world's nations. To build the ordered software, no more than ten employees would be required to work for no more than four weeks, perhaps as little as two weeks. Just as in *Mountain Bell*—where the company complained it would lose “irreplaceable services provided by key personnel” (Wilkison Decl. Ex. 6 at 24-25)—the burden for Apple here is not unreasonable. Moreover, the government has offered to compensate Apple for such costs that this Court determines have been actually incurred and are reasonably necessary for its efforts. *See New York Telephone Co.*, 434 U.S. at 175 (AWA order not unduly burdensome in part because it provided for reimbursement for the company's efforts); *Mountain Bell*, 616 F.2d at 1132 (same).

The government has always been willing to work with Apple to attempt to reduce any burden of providing access to the evidence on Farook's iPhone. *See Mountain Bell*, 616 F.2d at 1124 (noting parties' collaboration to reduce perceived burdens). Before seeking the Order, the government requested voluntary technical assistance from Apple, and provided the details of its proposal. (Supp. Pluhar Decl. ¶ 12.) Apple refused to discuss the proposal's feasibility and instead directed the FBI to methods of access that the FBI had already tried without success. (*Compare* Neuenschwander Decl. ¶¶ 54-61,

1 *with* Supp. Pluhar Decl. ¶ 12.) The government turned to the Court only as a last resort  
 2 and sought relief on narrow grounds meant to reduce possible burdens on Apple. The  
 3 Order allows Apple flexibility in how to assist the FBI. (Order ¶ 4.) The government  
 4 remains willing to seek a modification of the Order, if Apple can propose a less  
 5 burdensome or more agreeable way for the FBI to access Farook’s iPhone.<sup>9</sup> In contrast,  
 6 Apple makes little effort to explain which parts of the court’s order are burdensome, and  
 7 in what ways. Nor does Apple propose feasible alternatives that it would find less  
 8 burdensome.<sup>10</sup> Rather, relying on its exclusive knowledge of its software, Apple simply  
 9 asserts a single, complicated process, without any further elaboration.

10 In sum, Apple has failed to show that the only concrete burden it can identify—a  
 11 relatively low amount of technical labor—is undue, unreasonable, and noncompensable.

12 *c. Impinging on Apple’s Marketing of Its Products as Search-*  
 13 *Warrant-Proof Is Not an Undue Burden*

14 Apple next claims that complying with search warrants will undermine the  
 15 public’s trust in the security of the company’s products and services—a reformulation of  
 16 its concern, raised in the Eastern District of New York, that compliance will tarnish its  
 17 brand. This is the same argument made by the corporations and rejected by the courts in  
 18 *New York Telephone* and *Mountain Bell*, 616 F.2d at 1128. Mountain Bell argued that  
 19 complying with the order would jeopardize its relationship with its customers, and that it

20 <sup>9</sup> For the reasons discussed above, the FBI cannot itself modify the software on  
 21 Farook’s iPhone without access to the source code and Apple’s private electronic  
 22 signature. The government did not seek to compel Apple to turn those over because it  
 23 believed such a request would be less palatable to Apple. If Apple would prefer that  
 24 course, however, that may provide an alternative that requires less labor by Apple  
 25 programmers. *See In re Under Seal*, 749 F.3d 276, 281-83 (4th Cir. 2014) (affirming  
 26 contempt sanctions imposed for failure to comply with order requiring the company to  
 27 assist law enforcement with effecting a pen register on encrypted e-mail content which  
 28 included producing private SSL encryption key).

29 <sup>10</sup> For example, Apple suggests that—in complying with the Order—it would have  
 30 to undertake “substantial” programming to make the software suitable for “consumer  
 31 interaction.” (Neuenschwander Decl. ¶ 19.) But Apple does not explain why Farook’s  
 32 iPhone would need to be ready for “consumer interaction” simply to perform forensic  
 33 data extraction, and does not address the existence of available tools that Apple could  
 34 use to perform some of the ordered functions. (Perino Decl. ¶¶ 6.b, 25-29.)



1 could not continue to operate if the public perceived the company as an extension of law  
 2 enforcement. (Wilkison Decl. Ex. 6 at 32-33.) Those arguments did not persuade those  
 3 courts then, and they should not persuade this Court now. *Cf. Univ. of Pennsylvania v.*  
 4 *E.E.O.C.*, 493 U.S. 182, 195-98 (1990) (rejecting university’s argument that producing  
 5 certain information to the government would have a “chilling effect,” and declining to  
 6 recognize a business-interest privilege for withholding the information).

7 Apple also argues that the Order is unduly burdensome because it is in Apple’s  
 8 “basic interests” to make the data on its phones as secure as possible.<sup>11</sup> (Opp. 23.) The  
 9 company in *New York Telephone* similarly asserted in its Supreme Court merits briefing  
 10 that “[p]rotection of this privacy [*i.e.*, “the privacy of communications”] is fundamental  
 11 to the telephone business.” 1977 WL 189311, at \*2. It added that its “principal basis”  
 12 for opposing the order was “the danger of indiscriminate invasions of privacy.” *Id.* at  
 13 \*8. The Court rejected those arguments. 434 U.S. at 174. Moreover, programming  
 14 software is not “offensive to” Apple generally, *New York Telephone*, 434 U.S. at 174,  
 15 and here Apple’s own customer has asked to have the phone unlocked. Nor will  
 16 programming this particular software compromise the security of any Apple iPhone  
 17 other than Farook’s for reasons explained below. (*See infra* pp. 24-25.)

18 d. *Apple’s Speculation that Third Parties Could Be Harmed in*  
 19 *the Future if It Complies With the Order Does Not Establish an*  
*Undue Burden on Apple*

20 Apple speculates that if it submits to a lawful order to assist with a constitutional,  
 21 warranted search of a consenting customer’s phone in America, Apple will have no  
 22 choice but to help totalitarian regimes suppress dissidents around the globe, and  
 23 “hackers, criminals, and foreign agents” will have access to the data on millions of  
 24

25  
 26 <sup>11</sup> Apple insists that if this Court does not hold that it is a *per se* undue burden to  
 27 compel a corporation to act against its business interests, a parade of horrors will  
 28 ensue. (Opp. 26.) As noted above, this line of argument has been repeatedly rejected by  
 the courts. Moreover, the Fourth Amendment, the proximity and necessity factors, and  
 the courts’ ultimate discretion provide ample protection against executive overreaching.

1 iPhones. (Opp. 1-2, 28.) This putative public burden, Apple argues, is a basis to relieve  
 2 it from the Order. Apple’s fears are overblown for reasons both factual and legal.<sup>12</sup>

3 To begin with, many of the most compelling examples of cybercrime that Apple  
 4 describes involve not breaches of physical-device security, but rather breaches of  
 5 network security. That is the “the daily siege” of “hackers, cyber-criminals, and foreign  
 6 agents” with which the government and victims contend. (Opp. 1.) Nothing in the  
 7 Court’s Order affects Apple’s network security. Rather, the features at issue concern  
 8 only access to a physical device. Thus, for the government even to benefit from the  
 9 software set forth in the Order, it first had to recover Farook’s iPhone itself. (Perino  
 10 Decl. ¶¶ 6.c, 31-36.) That fact alone eliminates much of Apple’s worry.

11 Next, contrary to Apple’s stated fears, there is no reason to think that the code  
 12 Apple writes in compliance with the Order will ever leave Apple’s possession. Nothing  
 13 in the Order requires Apple to provide that code to the government or to explain to the  
 14 government how it works. And Apple has shown it is amply capable of protecting code  
 15 that could compromise its security. For example, Apple currently protects (1) the source  
 16 code to iOS and other core Apple software and (2) Apple’s electronic signature, which as  
 17 described above allows software to be run on Apple hardware. (Hanna Decl. Ex. DD at  
 18 62-64 (code and signature are “the most confidential trade secrets [Apple] has”).) *Those*  
 19 —which the government has *not* requested—are the keys to the kingdom. If Apple can  
 20 guard them, it can guard this.

21  
 22  
 23 <sup>12</sup> Apple speculates that there is no law-enforcement benefit to removing barriers  
 24 to unlocking an iPhone because criminals and terrorists will encrypt their data in other  
 25 ways. (Opp. 25.) If this reasoning were correct, there would be no purpose to wire-taps,  
 26 either. But the reasoning is flawed, for three reasons. *First*, as the wire-tap context  
 27 illustrates, just because criminals *can* add another layer of security (such as talking in  
 28 code), they do not always do so. *Second*, even if there are further layers of encryption,  
 the government may be able to pierce that encryption—but only if it can get into the  
 phone in the first place. *Third*, even assuming counterfactually that unlocking iPhones  
 would not be useful in the future due to changes in criminal and terrorist behavior, it is  
 useful *today* for gathering evidence related to the terrorist mass-murder in San  
 Bernardino.



1 Even if “criminals, terrorists, and hackers” somehow infiltrated Apple and stole  
 2 the software necessary to unlock Farook’s iPhone (Opp. 25), the *only* thing that software  
 3 could be used to do is unlock Farook’s iPhone. (Perino Decl. ¶¶ 6.a, 18-24.) Far from  
 4 being a master key, the software simply disarms a booby trap affixed to one door:  
 5 Farook’s. The software “will be coded by Apple with a unique identifier of the phone so  
 6 that the [software] would only load and execute on the SUBJECT DEVICE [*i.e.*,  
 7 Farook’s iPhone].” (Order ¶ 3.) This phone-specific limitation was not dreamed up by  
 8 the government, but instead employs Apple’s well-publicized security paradigm. A  
 9 “unique ID (ECID)” associated with each physical iPhone is incorporated into the  
 10 phone’s operating system. (Perino Decl. ¶ 20; Hanna Decl. Ex. K at 6.) “Adding the  
 11 ECID ‘personalizes’ the authorization for the requesting device.” (*Id.*) Apple has  
 12 designed its phones so that every operating system must pair with the phone’s ECID.  
 13 (Perino Decl. ¶¶ 18-24; Hanna Decl. Ex. K at 6 (describing how the Apple server “adds  
 14 the ECID” before it “signs” the iOS to be used for the upgrade).) The operating system  
 15 and ECID must correspond for the operating system to work. The ordered software  
 16 would rely upon the same limitation.

17 Apple implies that the code could be modified to run on other phones, but a  
 18 second Apple security layer prevents that from happening: Apple devices will only run  
 19 software that is electronically “signed” by Apple. (Hanna Decl. Ex. K at 6 (“only Apple-  
 20 signed code can be installed on a device”).) “Signing” the software described in the  
 21 Order will not release Apple’s signature to the government or anyone else—Apple signs  
 22 *all* publicly available iOS software, but that does not disclose the signature itself.  
 23 (Perino Decl. ¶¶ 9, 13-17, 24, 28.) And if the code were modified to run on a phone with  
 24 a different ECID, it would lack a valid digital signature. Without that signature, the code  
 25 would not run at all on *any* iOS phone with intact security. (*Id.*) Thus, it is simply not  
 26 plausible that Apple’s complying with the Order would cripple iPhone security.

27 Similarly misleading is Apple’s argument that the Order will force Apple to  
 28 provide access to data to foreign governments. As a legal matter, the Order does not—

1 *could not*—compel Apple to follow or disregard the laws of foreign countries. The  
2 pressure of foreign law on Apple flows from its decision to do business in foreign  
3 countries, not from the Order. Apple suggests that, as a practical matter, it will cease to  
4 resist foreign governments’ efforts to obtain information on iPhone users if this Court  
5 rules against it. It offers no evidence for this proposition, and the evidence in the public  
6 record raises questions whether it is even resisting foreign governments now. For  
7 example, according to Apple’s own data, China demanded information from Apple  
8 regarding over 4,000 iPhones in the first half of 2015, and Apple produced data 74% of  
9 the time. (Wilkison Decl. Ex. 8 at 3.) Apple appears to have made special  
10 accommodations in China as well: for example, moving Chinese user data to Chinese  
11 government servers, and installing a different WiFi protocol for Chinese iPhones. (*See*  
12 Wilkison Decl. Ex. 9 (reporting that in August 2014, Apple moved Chinese users’  
13 iCloud data onto state-owned servers); Ex. 10 (reporting that Apple produced a modified  
14 iPhone for sale in mainland China that used a “WAPI” WiFi standard as required by the  
15 Chinese government); Ex. 11 (reporting Apple was the first Western company to have its  
16 products use WAPI and “[t]hus, [Apple] is presumably sharing confidential information  
17 with the [Chinese] government”).) Such accommodations provide Apple with access to  
18 a huge, and growing, market. (Wilkison Decl. Ex. 12.) This Court’s Order changes  
19 neither the carrots nor the sticks that foreign governments can use on Apple. Thus, it  
20 does not follow that if America forgoes Apple’s assistance in this terrorism investigation,  
21 Apple will refuse to comply with the demands of foreign governments. Nor does it  
22 follow that if the Court stands by its Order, Apple must yield to foreign demands, made  
23 in different circumstances without the safeguards of American law.

24 Lawful process in America cannot be confined by potential lawless oppression  
25 elsewhere merely because a corporation chooses to manufacture and market its products  
26 globally, without regard to its host countries’ legal regimes. Apple identifies no case  
27 holding that such a “burden” is cognizable under the AWA. The concerns Apple raises  
28

are unproven, and in any event would not be an unreasonable burden on Apple created by the Order, but an inevitable consequence of Apple's own business decisions.

e. *Cumulative Future Compliance Costs Should Not Be Considered and Are, In Any Event, Compensable*

Next, Apple argues that the Order is unduly burdensome because, if it complies here, it is likely to face other AWA orders in the future. By accumulating its hypothetical future burdens, Apple suggests that because so much criminal evidence is hidden on its warrant-proof iPhones, it should not be compelled to assist in gathering evidence related to the terrorist attack in San Bernardino. (Opp. 26.) Apple is wrong.

To begin with, Apple has identified no precedent for considering possible prospective burdens as a basis for withholding a narrow AWA order now. Neither the Supreme Court in *New York Telephone* nor the Ninth Circuit in *Mountain Bell* considered prospective cumulative costs, even though "it [was] plain, given the Company's policy of refusing to render voluntary assistance in installing pen registers and the Government's determination to continue to utilize them, that the Company will be subjected to similar orders in the future." *New York Telephone*, 434 U.S. at 165 n.6. Instead, those courts looked only at the costs associated with the particular order. *Id.* at 174; *Mountain Bell*, 616 F.2d at 1133. This follows logically from the individualized, fact-intensive nature of the AWA inquiry. Apple's future costs—which can be compensated in future cases—are mere guesswork, especially since, without knowing the facts, there is no way to predict how the courts in hypothetical future cases will weigh the three *New York Telephone* factors.<sup>13</sup>

Moreover, Apple has proven itself more than able to comply with a large volume of law-enforcement requests. Apple has a dedicated team for doing so (Olle Decl. ¶ 2), and it has published guidelines on how legal process will be handled (Wilkison Decl. Ex.

<sup>13</sup> Apple is reportedly already working to re-design the iPhone to preclude compliance with any similar future court orders, which is another reason to question its claimed cumulative costs *and* its assertion that coding is an undue burden for the company. (Wilkison Decl. Ex. 14.)

13). In the first half of 2015 alone, Apple handled 27,000 “device requests”—often covering multiple devices—and provided data approximately 60% of the time. (Wilkison Decl. Ex. 8 at 3-4.) If Apple can provide data from thousands of iPhones and Apple users to China and other countries, it can comply with the AWA in America. (*Id.*) This is not speculation because, in fact, Apple complied for years with American court orders to extract data from passcode-locked iPhones, dedicating infrastructure and personnel in order to do so. (Wilkison Decl. Ex. 14 at 2-3; *id.* Ex. 16 at 3 n.3; Hanna Decl. Ex. DD at 56.) It never objected or sought compensation. (*Compare* Olle Decl. ¶ 13, *with* Hanna Decl. Ex. DD 58 (“[W]e’ve never required compensation.”).) Apple can handle, and has handled, this burden.<sup>14</sup>

In sum, the only concrete, cognizable burdens Apple can identify are reasonable, not undue, and the remaining burdens are speculative and unrecognized by precedent.

### 3. *Apple’s Assistance Is Necessary*

Without Apple’s assistance, the government cannot carry out the search of Farook’s iPhone authorized by the search warrant. Apple has ensured that its assistance is necessary by requiring its electronic signature to run any program on the iPhone. Even if the Court ordered Apple to provide the government with Apple’s cryptographic keys and source code, Apple itself has implied that the government could not disable the requisite features because it “would have insufficient knowledge of Apple’s software and design protocols to be effective.” (Neuenschwander Decl. ¶ 23.)

---

<sup>14</sup> Apple also complains of having “to testify about this back door as a government witnesses at trial.” (Opp. 26). “The giving of testimony and the attendance upon court or grand jury in order to testify are public duties which every person within the jurisdiction of the government is bound to perform upon being properly summoned.” *Blair v. United States*, 250 U.S. 279, 281 (1919). Moreover, Apple makes no attempt to quantify such costs, instead relying on the implication that the crown jewels of its intellectual property would be released to the world in court. Experience suggests that this is more of a fear than a reality. During the years when Apple followed court orders to extract data from passcode-locked iPhones, the vast majority of affiliated criminal cases were resolved without any need for Apple to testify. (Hanna Decl. Ex. DD 24-25.) Moreover, as Apple conceded, in cases in which testimony from an Apple representative was necessary, no intellectual property was lost. (*Id.* 25.)

1           Rather than acknowledge this point, Apple instead blames the San Bernardino  
2 County Department of Public Health and the FBI. Apple argues that the FBI could have  
3 gained access to some of the information via a forced backup to Farook's iCloud  
4 account, but since the FBI changed the iCloud password to gain quick access to what  
5 was stored in previous backups in the immediate aftermath of the San Bernardino  
6 shooting, this path was blocked. (Opp. 11.) That is both untrue and irrelevant.

7           For several reasons, a forced iCloud backup would not have been successful even  
8 if the password had remained unchanged. Farook's iPhone was found powered off.  
9 (Supp. Pluhar Decl. ¶ 2.) Subsequent testing has revealed that once powered off, an  
10 iPhone will not back itself up to an iCloud account unless and until it has been unlocked  
11 at least once by use of the passcode. (Perino Decl. ¶¶ 6.d, 37-39.) Moreover, the  
12 evidence on Farook's iCloud account suggests that he had already changed his iCloud  
13 password himself on October 22, 2015—shortly after the last backup—and that the auto-  
14 backup feature was disabled. (Pluhar Decl. ¶ 8; Supp. Pluhar Decl. ¶ 9.) A forced  
15 backup of Farook's iPhone was never going to be successful, and the decision to obtain  
16 whatever iCloud evidence was immediately available via the password change was the  
17 reasoned decision of experienced FBI agents investigating a deadly terrorist conspiracy.

18           Moreover, even if—contrary to how Apple built and designed it—Farook's  
19 iPhone could have been forced to sync to Apple's iCloud network, that would not be an  
20 adequate substitute to unlocking and searching the phone itself. Both the FBI's testing  
21 and Apple's security documentation show that entire categories of evidence—including  
22 device-level data such as the "keyboard cache" (which records recent keystrokes)—  
23 reside only on the iPhone and not on an iCloud backup, and that some of the backup data  
24 would still have been encrypted. (Supp. Pluhar Decl. ¶ 10.) But that data remains on the  
25 iPhone. Thus, even with a full set of backups, the government still would have needed to  
26 search the phone itself in order to leave no stone unturned in this important investigation.

27           Most importantly, even assuming counterfactually that something could have been  
28 recovered through a forced iCloud backup, there have been no backups since October 19,

1 2015, and Apple concedes there is no way to force a backup now. Thus, the only way to  
2 recover *any* subsequent data—whether subject to backup or otherwise—is to unlock  
3 Farook’s iPhone. And for the FBI to do that, Apple must remove the barriers it put on  
4 that phone.

5 Apple insists that under *New York Telephone*, the government must show “there is  
6 no conceivable way” to search Farook’s iPhone without Apple’s assistance, and  
7 contends that the government has not borne this burden. (Opp. 30); 434 U.S. at 174.  
8 Apple’s quoting of *New York Telephone* lacks context. There, the FBI could install the  
9 pen register on its own—just not in an “inconspicuous” location. *Id.* at 161. Moreover,  
10 there is no indication that the FBI first enlisted the entire federal government in search of  
11 investigative alternatives. *Id.* at 175 (“The FBI . . . was unable to find a location where *it*  
12 could install its own pen registers without tipping off the targets of the investigation.”  
13 (emphasis added)). The broader reasoning of *New York Telephone* further refutes an  
14 absolute necessity standard: the Court expressly relied upon the “necessary *or*  
15 *appropriate*” language in the All Writs Act. *Id.* at 172-74. Regardless, even if absolute  
16 necessity were required, the undisputed evidence is that the FBI cannot unlock Farook’s  
17 phone without Apple’s assistance. (Wilkison Decl. Ex. 16 at 2-3; Pluhar Decl. ¶ 9.)

18 \* \* \*

19 The “definite and concrete” facts of *this* case—as opposed to the “hypothetical or  
20 abstract” future scenarios conjured up by Apple, *see Corsi*, 326 U.S. at 93—amply  
21 support the Court’s Order. Apple deliberately established a security paradigm that keeps  
22 Apple intimately connected to its iPhones. This same paradigm makes Apple’s  
23 assistance necessary for executing the lawful warrant to search Farook’s iPhone. Such  
24 assistance imposes a burden that is not unreasonable, particularly for a company of  
25 Apple’s wealth, size, and technical prowess. The Order does no more than require Apple  
26 to unknot some of the tangle it has made, so that the court-authorized investigation into  
27 Farook’s iPhone can proceed.



**D. The Order Does Not Implicate, Let Alone Violate, the First and Fifth Amendments**

Apple begins its Opposition by insisting that the issues in this case should be left to Congress (Opp. 9), and ends by insisting that the Constitution takes those issues off the table (Opp. 32-34). Not so. The Order is constitutional, notwithstanding Apple's assertion of corporate speech rights and *Lochner*-era substantive due process.<sup>15</sup>

*1. Incidentally Requiring a Corporation to Add Functional Source Code to a Commercial Product Does Not Violate the First Amendment*

Apple asserts that functional source code in a corporation's commercial product is core protected speech, such that asking it to modify that software on one device—to permit the execution of a lawful warrant—is compelled speech in violation of the First Amendment. This claim “trivializes the freedom protected in *Barnette* and *Wooley*.”<sup>16</sup> *See Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.*, 547 U.S. 47, 62 (2006).

Before reaching the specifics of Apple's claim, it is important to start with a threshold observation: the “essential operations” of the American legal system rest upon people sometimes having to say things that they would rather not say—such as when a witness is subpoenaed and sworn to speak the whole truth and nothing but the truth. *West Virginia Bd. of Ed. v. Barnette*, 319 U.S. 624, 645 (1943) (Murphy, J., concurring) (compelled speech doctrine inapplicable to “essential operations of government” such “as in the case of compulsion to give evidence in court”); *see also* *Murphy v. Waterfront*

---

<sup>15</sup> The search of a smartphone *does* implicate the Fourth Amendment, *see Riley*, 134 S. Ct. at 2484, but the government has doubly satisfied the Fourth Amendment by obtaining (1) a warrant, *id.*, and (2) the consent of the phone's owner. Moreover, Apple cannot assert any privacy interests of the phone's deceased user, the terrorist Farook. *See Simmons v. United States*, 390 U.S. 377, 389 (1968) (“[R]ights assured by the Fourth Amendment are personal rights, and that they may be enforced by exclusion of evidence only at the instance of one whose own protection was infringed by the search.”).

<sup>16</sup> Apple rightly does not attempt to claim standing to assert the First Amendment rights of iPhone users whose phones are not being searched. To the extent *amici* raise such arguments, they are untethered to the issues actually before the Court and, in any event, foreclosed by the Supreme Court's ruling in *Zurcher v. Stanford Daily*, 436 U.S. 547, 563-65 (1978), rejecting a newspaper's claim that a search of its records would chill its speech rights because it would “resort to self-censorship to conceal its possession of information of potential interest to the police.”

1 *Comm’n of New York Harbor*, 378 U.S. 52, 93-94 (1964) (“Among the necessary and  
 2 most important of the powers of . . . the Federal Government to assure the effective  
 3 functioning of government in an ordered society is the broad power to compel residents  
 4 to testify in court or before grand juries or agencies.”), *abrogated on other grounds by*  
 5 *United States v. Balsys*, 524 U.S. 666 (1998). This form of “compelled speech” runs  
 6 throughout both the criminal and civil justice systems, from grand jury and trial  
 7 subpoenas to interrogatories and depositions. *See, e.g.*, Apple Inc.’s Motion to Compel  
 8 in *Apple Inc. v. Samsung Electronics*, Docket No. 467 in Case No. 11-cv-1846-LHK, at  
 9 11 (N.D. Cal. Dec. 8, 2011) (Apple’s seeking court order compelling Samsung to  
 10 produce source code to facilitate its compelled deposition of witnesses about that source  
 11 code). If the First Amendment swept as broadly as Apple suggests, there would be no  
 12 need, for example, for the Fifth Amendment’s privilege against self-incrimination.

13 Apple’s claim is particularly weak because it does not involve a person being  
 14 compelled to speak publicly, but a for-profit corporation being asked to modify  
 15 commercial software that will be seen only by Apple. There is reason to doubt that  
 16 functional programming is even entitled to traditional speech protections. *See, e.g.*,  
 17 *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (recognizing  
 18 that source code’s “functional capability is not speech within the meaning of the First  
 19 Amendment”). “[T]hat [programming] occurs at some level through expression does not  
 20 elevate all such conduct to the highest levels of First Amendment protection. Doing so  
 21 would turn centuries of our law and legal tradition on its head, eviscerating the carefully  
 22 crafted balance between free speech and permissible government regulation.” *United*  
 23 *States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1128-29 (N.D. Cal. 2002).

24 To the extent Apple’s software includes expressive elements—such as variable  
 25 names and comments—the Order permits Apple to express whatever it wants, so long as  
 26 the software functions. *Cf. Karn v. United States Department of State*, 925 F. Supp. 1, 9-  
 27 10 (D.D.C. 1996) (assuming, without deciding, that source code was speech because it  
 28 had English comments interspersed). Indeed, the Order’s “broad requirements” do “not



1 dictate any specific message,” but leave it open to Apple to decide how to develop the  
2 code. *See Envtl. Def. Ctr., Inc. v. U.S. E.P.A.*, 344 F.3d 832, 849-51 (9th Cir. 2003).  
3 And even assuming, *arguendo*, that the Order compels speech-like programming, there  
4 is no audience: Apple’s code will be developed in the utmost secrecy and will never be  
5 seen outside the corporation. *Cf. Full Value Advisors, LLC v. S.E.C.*, 633 F.3d 1101,  
6 1108-09 (D.C. Cir. 2011) (“constitutional concerns” with compelled public speech are  
7 not triggered when government commission “is [the] only audience”); *United States v.*  
8 *Sindel*, 53 F.3d 874, 878 (8th Cir. 1995) (lesser concern where compelled speech lacks  
9 “public dissemination”). This stands in stark contrast to the cases cited by Apple, in  
10 which software creators were forbidden from publicly sharing what they had written.  
11 For all of these reasons, the Order simply does not compel speech.

12 At most, the Order compels conduct—namely, the removal of barriers from  
13 Farook’s iPhone—with an incidental effect on “speech” (*i.e.*, programming). That does  
14 not amount to a First Amendment violation for the reasons explained by the Supreme  
15 Court in *Rumsfeld*, which rejected a First Amendment challenge to the requirement that  
16 law schools host and promote military recruitment even if the schools objected to  
17 military policy. Like in *Rumsfeld*, “[t]he compelled speech . . . is plainly incidental to  
18 the [Order’s] regulation of conduct.” 547 U.S. at 62. The Order simply requires Apple  
19 to remove barriers from Farook’s phone. That is conduct, not speech. As the Supreme  
20 Court explained, “Congress, for example, can prohibit employers from discriminating in  
21 hiring on the basis of race. The fact that this will require an employer to take down a  
22 sign reading ‘White Applicants Only’ hardly means that the law should be analyzed as  
23 one regulating the employer’s speech rather than conduct.” *Id.*

24 Further, how Apple’s software is engineered “is not inherently expressive.” *Id.* at  
25 64. Code determining how many retries a user is permitted before the data on an iPhone  
26 is permanently lost “lack[s] the expressive quality of a parade, a newsletter, or the  
27 editorial page of a newspaper.” *Id.* As in *Rumsfeld*, any expressive dimension to  
28 Apple’s compliance with the Order arises “only because [Apple] accompanied [its]

1 conduct with speech explaining it.” *Id.* at 66. Presumably, Apple will respond that if it  
 2 modifies Farook’s iPhone to allow the government access to the phone, it “could be  
 3 viewed as sending the message that [it] see[s] nothing wrong with [such access], when  
 4 [it] do[es].” *Id.* at 64-65. But the Supreme Court derided that argument in *Rumsfeld*,  
 5 explaining that “[n]othing about recruiting suggests that law schools agree with any  
 6 speech by recruiters, and nothing in the Solomon Amendment restricts what the law  
 7 schools may say about the military’s policies.” *Id.* at 65. So too here. And just as in  
 8 *Rumsfeld*, the public “can appreciate the difference between speech [Apple] sponsors”  
 9 and code Apple develops “because [it is] legally required to do so.” *Id.* It is extremely  
 10 unlikely that anyone could understand Apple to be expressing a message of hostility to  
 11 “data security and the privacy of citizens” (Opp. 33), “given both the nature of [Apple’s]  
 12 activity and the factual context and environment in which it was undertaken.” *Jacobs v.*  
 13 *Clark Cty. Sch. Dist.*, 526 F.3d 419, 438 (9th Cir. 2008).

14 Even if, despite the above, the Order placed some burden on Apple’s ability to  
 15 market itself as hostile to government searches, that would not establish a First  
 16 Amendment violation because the Order “promotes a substantial government interest  
 17 that would [otherwise] be achieved less effectively.” *Rumsfeld*, 547 U.S. at 67. There is  
 18 no question that searching a terrorist’s phone—for which a neutral magistrate has found  
 19 probable cause—is a compelling government interest. *See Branzburg v. Hayes*, 408 U.S.  
 20 665, 700 (1972) (recognizing that “the investigation of a crime” and “securing the  
 21 safety” of citizens are “fundamental” interests for First Amendment purposes). As set  
 22 forth above, the FBI cannot search Farook’s iPhone without Apple’s assistance, and  
 23 Apple has offered no less speech-burdensome manner for providing that assistance.

24 For all of these reasons, Apple’s First Amendment claim must fail.

## 25 2. *There Is No Due Process Right Not to Develop Source Code*

26 Apple lastly asserts that the Order violates its Fifth Amendment right to due  
 27 process. Apple is currently availing itself of the considerable process our legal system  
 28 provides, and it is ludicrous to describe the government’s actions here as “arbitrary.”

(Opp. 34); *see County of Sacramento v. Lewis*, 523 U.S. 833, 846-49 (1998). If Apple is asking for a *Lochner*-style holding that businesses have a substantive due process right against interference with its marketing strategy or against being asked to develop source code, that claim finds no support in any precedent, let alone “in the traditions and conscience of our people,” “the concept of ordered liberty,” or “this Nation’s history.” *Washington v. Glucksberg*, 521 U.S. 702, 721 (1997).

### III. CONCLUSION

The All Writs Act empowered this Court to issue the Order, just as it empowered a court to order a corporation to engage in computer programming and technical assistance in *Mountain Bell*. As the Supreme Court has repeatedly recognized—and as Congress’s repeated reaffirmation and expansion of the Act have confirmed—the Act’s flexibility in confronting new problems shows the Framers’ foresight and genius, not a blind spot. As the decades since *New York Telephone* have shown, as indeed the centuries since 1789 have proven, courts’ exercise of power under the Act does not lead to a headlong tumble down a slippery slope to tyranny. That is because the Act itself—by relying upon the sound discretion of federal judges and by being subordinate to *specific* congressional legislation addressing the *particular* issue—builds in the necessary safeguards. Moreover, the Fourth Amendment, which Apple concedes has been satisfied here, protects against unreasonable privacy invasions.

In short, the limits Apple seeks are already found in the Constitution, the Act, and the three branches of government: congressional legislation, executive restraint, and judicial discretion. The government respectfully submits that *those* authorities should be entrusted to strike the balance between each citizen’s right to privacy and all citizens’ right to safety and justice. The rule of law does not repose that power in a single corporation, no matter how successful it has been in selling its products.

Accordingly, the government respectfully requests that this Court DENY Apple’s motion to vacate this Court’s February 16, 2016 Order, and compel Apple to assist the FBI in unlocking Farook’s iPhone.