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

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

MARC J. ZWILLINGER*
marc@zwillgen.com
JEFFREY G. LANDIS*
jeff@zwillgen.com
ZWILLGEN PLLC
1900 M Street N.W., Suite 250
Washington, DC 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298
*Admitted *Pro Hac Vice*

Attorneys for Apple Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

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

ED No. CM 16-10 (SP)

APPLE INC.'S REPLY TO GOVERNMENT'S OPPOSITION TO APPLE INC.'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH

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

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

This reply is based upon the attached memorandum of points and authorities, the declarations of Nicola T. Hanna, Craig Federighi, Erik Neuenschwander, and Robert Ferrini filed concurrently herewith, the files and records in this case, and such further evidence and argument as the Court may permit.

Dated: March 15, 2016

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

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

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

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

Marc J. Zwillinger *
Jeffrey G. Landis *
ZwillGen PLLC
1900 M Street N.W., Suite 250
Washington, DC 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298
*Admitted *Pro Hac Vice*

Attorneys for Apple Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES *(continued)*

TABLE OF AUTHORITIES *(continued)*

Page(s)

TABLE OF AUTHORITIES *(continued)*

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The Justice Department and FBI are seeking an order from this Court that would force Apple to create exactly the kind of operating system that Congress has thus far refused to require. They are asking this Court to resolve a policy and political issue that is dividing various agencies of the Executive Branch as well as Congress. This Court should reject that request, because the All Writs Act does not authorize such relief, and the Constitution forbids it.[1]

The All Writs Act cannot be stretched to fit this case because to do so "would be to usurp the legislative function and to improperly extend the limited federal court jurisdiction." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1290 (9th Cir. 1979). The government attempts to rewrite history by portraying the Act as an all-powerful magic wand rather than the limited procedural tool it is. As theorized by the government, the Act can authorize any and all relief except in two situations: (1) where Congress enacts a specific statute prohibiting the precise action (*i.e.*, says a court may not "order a smartphone manufacturer to remove barriers to accessing stored data on a particular smartphone," Opp. 11), or (2) where the government seeks to "arbitrarily dragoon[]" or "forcibly deputize[]" "random citizens" off the street. Opp. 5, 16. Thus, according to the government, short of kidnapping or breaking an express law, the courts can order private parties to do virtually anything the Justice Department and FBI can dream up. The Founders would be appalled.

Furthermore, the Justice Department and FBI argue that this Court must decide the issue in a vacuum, without regard to either the swirling national debate about

[1] The government's brief assails Apple's intentions and motivations. We do not intend to respond in kind. As FBI Director Comey testified, "there are no demons [here]." Ex. EE at 11 [FBI Director James Comey, *Encryption Tightrope: Balancing Americans' Security and Privacy*, Hearing on Encryption Security and Privacy Before the H. Comm. on the Judiciary (Mar. 1, 2016) ("*Encryption Hr'g*")]. Our goal is to focus on the facts and law. (Unless otherwise indicated, all referenced exhibits are attached to the Supplemental Declaration of Nicola T. Hanna filed concurrently herewith.)

mandating a back door or the dangers to the security and privacy of millions of citizens posed by the relief they seek on behalf of the United States. But to determine whether this is an issue capable of judicial resolution under the All Writs Act and the Constitution, the Court not only can consider this broader context, it must do so. Indeed, the Justice Department and FBI are asking this Court to adopt their position even though numerous current and former national security and intelligence officials flatly disagree with them. *See, e.g.*, Ex. FF [Spencer Ackerman & Danny Yadron, *US Defense Chief Tells Silicon Valley: "Encryption Is Essential,"* Guardian (Mar. 2, 2016)] (quoting Defense Secretary Ashton Carter: "[D]ata security, including encryption, is absolutely essential to us. . . . I'm not a believer in backdoors . . . ."); Ex. GG [Michael D. Shear & David E. Sanger, *Competing Interests on Encryption Divide Top Obama Officials*, N.Y. Times (Mar. 5, 2016)] ("Driven by competing and sometimes clashing interests about privacy, national security and the economy, some of the president's most senior aides are staking out a variety of positions on the issue."); Ex. HH [Tom DiChristopher, *US Safer with Fully Encrypted Phones*, CNBC (Feb. 23, 2016)] (quoting former NSA and CIA Director Michael Hayden: "America is more secure—America is more safe—with unbreakable end-to-end encryption.").

It has become crystal clear that this case is not about a "modest" order and a "single iPhone," Opp. 1, as the FBI Director himself admitted when testifying before Congress two weeks ago. Ex. EE at 35 [FBI Director James Comey, *Encryption Hr'g*] ("[T]he broader question we're talking about here goes far beyond phones or far beyond any case. This collision between public safety and privacy—the courts cannot resolve that."). Instead, this case hinges on a contentious policy issue about how society should weigh what law enforcement officials want against the widespread repercussions and serious risks their demands would create. "Democracies resolve such tensions through robust debate" among the people and their elected representatives, Dkt. 16-8 [Comey, *Going Dark*], not through an unprecedented All Writs Act proceeding.

This case arises in a difficult context after a terrible tragedy. But it is in just such highly-charged and emotional cases that the courts must zealously guard civil liberties and the rule of law and reject government overreaching. This Court should therefore deny the government's request and vacate the order.

II. ARGUMENT

A. The Government Misconceives The All Writs Act's Scope And Purpose.

The government portrays the All Writs Act as a "broad," "venerable," "fluid," "adaptable" font of virtually unlimited authority empowering courts to issue any and all orders that the government requests in the pursuit of "justice." Opp. 3–5. As the government tells it, courts can wield the "flexible power" conferred by the Act until "Congress expressly takes it away." Opp. 10. This is an exercise in wishful thinking, not statutory interpretation.

The Act authorizes courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). The Act's reference to "writs" "agreeable to the usages and principles of law" refers to "traditional writs that have not been altered or abolished by some other statute." *Lowery v. McCaughtry*, 954 F.2d 422, 423 (7th Cir. 1992). "In determining what auxiliary writs are 'agreeable to the usages and principles of law,' [the Court] look[s] first to the common law." *United States v. Hayman*, 342 U.S. 205, 221 n.35 (1952); *see also* John W. Kyle, *Nature and Origin of Writs Under the Common Law*, 24 Miss. L.J. 1, 1 (1952) ("Practically all of the writs which are now in use in England and America have a common law origin.").

Because the Act is grounded in the common law, it is "not a grant of plenary power to the federal courts." *Plum Creek Lumber Co.*, 608 F.2d at 1289. Nor does the Act "give the district court a roving commission" to order private parties to assist the government. *Id.* Rather, it "function[s] as a 'gap filler,'" *In re Apple, Inc.*, -- F. Supp. 3d --, 2016 WL 783565, at *8 (E.D.N.Y. Feb. 29, 2016), that "suppl[ies] the courts with the instruments needed to perform their duty," *Harris v. Nelson*, 394 U.S. 286, 300

(1969). For example, Congress has authorized courts to issue "the writ of *habeas corpus ad testificandum*," such that a "court may direct the custodian to produce the prisoner in court as a witness." *Ivey v. Harney*, 47 F.3d 181, 183 (7th Cir. 1995). But "[w]hat happens if the testimony takes two days? Where does the prisoner stay overnight? . . . The statute does not say; neither, however, does it subtract from the court's common law powers to control such details." *Id.* The Act would fill such a gap as a "residual source of authority" authorizing the court "to issue writs that are not otherwise covered by [the] statute." *Clinton v. Goldsmith*, 526 U.S. 529, 537–38 (1999) (citation omitted). However, the Act "does not authorize [courts] to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985).

The government seeks an order here that is neither grounded in the common law nor authorized by statute. Indeed, the government has not pointed to *any* writ available at common law that would require a private non-party to perform burdensome forensics work, create new software, or compel speech to assist law enforcement.[2] The government misquotes *Bank of the United States v. Halstead*, 23 U.S. (10 Wheat.) 51 (1825), for the proposition that "'[t]he operation of [the Act]'" should not be limited "'to that which it would have had in the year 1789.'" Opp. 3 (misquoting *Halstead*, 23 U.S. (10 Wheat.) at 62) (alterations are the government's). But what the Court actually said was that the "operation of *an execution*"—the ancient common law writ of "*venditioni exponas*"—is not limited to that "which it would have had in the year 1789." 23 U.S. (10 Wheat.) at 62 (emphasis added); *see also id.* at 55 ("That executions are

[2] The government contends that Chief Justice Marshall once ordered a third party to "provide decryption services" to the government. Opp. 20 (citing *United States v. Burr*, 25 F. Cas. 38 (C.C.D. Va. 1807) (No. 14692E)). He did nothing of the sort, and the All Writs Act was not even at issue in *Burr*. In that case, Aaron Burr's secretary declined to state whether he "understood" the contents of a certain letter written in cipher, on the ground that he might incriminate himself. 25 F. Cas. at 39. The Court held that the clerk's answer as to whether he *understood* the cipher could not incriminate him, and the Court thus held that "the witness may answer the question now propounded"—*i.e.*, whether he understood the letter. *Id.* at 40. The Court did not require the clerk to decipher the letter.

among the writs hereby authorized to be issued, cannot admit of a doubt . . . ."). The narrow holding of *Halstead* was that the Act (and the Process Act of 1792) allowed courts "to *alter the form of the process of execution*." *Id*. at 54–55 (emphasis added) (courts are not limited to the *form* of the writ of execution "in use in the Supreme Courts of the several States in the year 1789"). The limited "power given to the Courts over their process is no more than authorizing them to regulate and direct the conduct of the Marshal, in the execution of the process." *Id.* at 61; *cf. Beers v. Haughton*, 34 U.S. (9 Pet.) 329, 359–60 (1835).

The authority to alter the *process* by which courts issue traditional common law writs is *not* authority to invent entirely new writs with no common law analog.[3] But that is precisely what the government is asking this Court to do: The Order requiring Apple to create software so that the FBI can hack into the iPhone has no common law analog. *See Ivey*, 47 F.3d at 185 (reversing order issued under the All Writs Act because "[n]othing in the common law supports an order directing a third party to provide free services that facilitate litigation"). Indeed, the Order is akin to an injunction directing specific performance of a personal services contract, a remedy the common law specifically disfavored. *See Barndt v. County of Los Angeles*, 211 Cal. App. 3d 397, 403-04 (1989) ("It has long been established that a contract to perform personal services cannot be specifically enforced . . . .") (citing *Poultry Producers of S. Cal., Inc. v.*

[3] The government's reliance on *Price v. Johnston*, 334 U.S. 266 (1948) (Opp. 4), is equally misplaced. Like *Halstead*, *Price* involved the form of a foundational common law writ—the writ of *habeas corpus*. 334 U.S. at 269. The Court recognized that the federal courts, "in issuing a writ of *habeas corpus* . . . [are not] necessarily confined to the precise forms of that writ in vogue at the common law or in the English judicial system." *Id.* at 282 (emphasis added). The Court thus held that the Act gave a court of appeals the power "to command that a prisoner be brought before it so that he may argue his own appeal in a case involving his life or liberty," even though the *habeas* writ had not been used for that particular purpose at common law. *Id.* at 278, 281-82. The Court's statement that the term "law" is "unlimited by the common law or the English law" referred only to the *form* of the writ of *habeas corpus*. *Id.* at 282 ("[W]e do not believe that the *forms of the habeas corpus* writ authorized by [the All Writs Act] are only those recognized in this country in 1789.") (emphasis added). The Court did *not* suggest that the Act provides authority to make new law or invent new writs.

Barlow, 189 Cal. 278, 288 (1922)); *see also* Restatement (Second) of Contracts § 367(1) ("A promise to render personal service will not be specifically enforced."). Courts have been especially reluctant to order specific performance where, as here, the "duties" of the performing party "involve skill, personal labor, and cultivated judgment." *Marble Co. v. Ripley*, 77 U.S. (10 Wall.) 339, 358 (1870).

The government nevertheless contends that because this Court issued a valid search warrant, it can order innocent third parties to provide *any* service the government deems "necessary" or "appropriate" to accomplish the search. Opp. 5. But that "broad" and "flexible" theory of the All Writs Act has no limiting principle. *See Ivey*, 47 F.3d at 185 (considering several "hypothetical parallel[s]" showing that petitioner's reading of the Act would allow the court to issue any number of orders not allowed at common law). Indeed, it is telling that the government fails even to confront the hypotheticals posed to it (*e.g.*, compelling a pharmaceutical company to manufacture lethal injection drugs, Dkt. 16 ("Mot.") at 26), or explain how there is any conceivable daylight between GovtOS today, and LocationTrackingOS and EavesdropOS tomorrow.[4]

Finally, the government sidesteps limitations imposed by the political question doctrine by assailing a strawman (Opp. 7–8), ignoring governing law and salient facts. First, the government cites case law reciting "the general rule" (which Apple does not dispute) "that 'the Judiciary has a responsibility to decide cases properly before it'" (Opp. 7 (citations omitted)) without explaining why *this* case is "properly before [the court]" within the meaning of the cited precedents. The government then conspicuously omits any mention of five of the six political question factors, asserting only that, generally, "'judicially discoverable and manageable standards'" exist here because

[4] The government is adept at devising new surveillance techniques. *See, e.g.*, *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (rejecting government's attempt to "hack" a computer to "surreptitiously install[] software designed . . . to generate user photographs and location information over a 30 day period"); *Company v. United States*, 349 F.3d 1132 (9th Cir. 2003) (rejecting government's attempt to use vehicle's OnStar system as bugging device).

"AWA standards" have long been litigated. Opp. 7–8 (quoting *Baker v. Carr*, 369 U.S. 186, 217 (1962)). But Supreme Court precedent makes clear that the mere fact that courts have discerned manageable standards to provide relief under a given law in the past—in response to distinct claims and under distinct circumstances—is not dispositive of the judicial manageability of all future claims seeking relief under the same law.[5] And as the Chairman of the House Judiciary Committee has recognized, "[i]t is clear that [this case] illustrate[s] . . . [a] dynamic policy question . . . that is too complex to be left to the courts and must be answered by Congress." Ex. EE at 3 [*Encryption Hr'g*].

B. The Government Cannot Invoke The All Writs Act Here.

1. The Government Cannot Use The Act To Circumvent CALEA.

The government seeks authority that Congress has expressly and impliedly rejected through CALEA, 47 U.S.C. § 1001 *et seq*. CALEA defines the circumstances under which private companies must create systems to assist law enforcement in its investigatory efforts, as well as the circumstances where such providers are not and cannot be required to build programs and systems to enable law enforcement access.[6] Contrary to the government's assertion that its request merely "brush[es] up against similar issues" to CALEA (Opp. 11), CALEA, in fact, has three critical limitations—two of which the government ignores entirely—that preclude the relief the government

[5] The Supreme Court has held, for instance, that "no judicially discernible and manageable standards" existed to decide a gerrymandering claim asserted on particular facts under 42 U.S.C. § 1983 and the Fourteenth Amendment, *Vieth v. Jubelirer*, 541 U.S. 267, 281 (2004), even though the Court had previously held in *Baker*—where plaintiffs invoked the same provisions—that "[j]udicial standards under the Equal Protection Clause are well developed and familiar," 369 U.S. at 226. *See also Vieth*, 541 U.S. at 311 (Kennedy, J., concurring).

[6] In the face of CALEA, the government claims that "a distinct area of law should not 'curtail[] the government's powers in domestic law enforcement' *under the AWA*," quoting *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc). Opp. 11 (emphasis added). This misleading juxtaposition of a quote from *Koyomejian* with the government's words—"under the AWA"—makes it seem as if the Ninth Circuit applied the All Writs Act, when it did not. *See* 970 F.2d at 542 (holding that since the Foreign Intelligence Surveillance Act does not regulate silent domestic video surveillance, such surveillance need only be authorized under Fed. R. Crim. P. 41 and consistent with the Fourth Amendment).

seeks. Mot. 15–19. First, CALEA prohibits law enforcement agencies from requiring "electronic communication service" providers to adopt "any specific design of equipment, facilities, services, features, or system configurations . . . ." 47 U.S.C. § 1002(b)(1)(A). The term "electronic communication service" provider is broadly defined to encompass Apple. *Id.* § 1001(1) (incorporating the definitions set forth in 18 U.S.C. § 2510); 18 U.S.C. § 2510(15) ("any service which provides to users thereof the ability to send or receive wire or electronic communications"). Apple is an "electronic communication services" provider for purposes of the very services at issue here because Apple's software allows users to "send or receive . . . communications" between iPhones through features such as iMessage and Mail. *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008) (providers of text messaging and email services are electronic communication service providers) *rev'd on other grounds*, *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010) ; *see also Application of the U.S. for an Order*, 349 F.3d 1132, 1138–41 (9th Cir. 2003) (entity is electronic communication service provider even if it depends on another, such as telephone company, for ability to provide services).

The government acknowledges that FaceTime and iMessage are electronic communication services, but asserts that this fact is irrelevant because "the Court's order does not bear at all upon the operation of those programs." Opp. 12 n.3. Not so. The passcode Apple is being asked to circumvent is a feature of the same Apple iOS that runs FaceTime, iMessage, and Mail, because an integral part of providing those services is enabling the phone's owner to password-protect the private information contained within those communications.[7] More importantly, the very communications to which law enforcement seeks access are the iMessage communications stored on the phone. *See* Dkt. 1 [Gov't Mot. to Compel] at 1. And, only a few pages after asserting

[7] The government's assertion that the order does not dictate "any specific design," Opp. 12 (quoting 47 U.S.C. § 1002(b)(1)), is baseless given that the order commands Apple to design specific new software with specific capabilities.

that "the Court's order does not bear at all upon the operation of" FaceTime and iMessage for purposes of the CALEA analysis (Opp. 12 n.3), the government spends several pages seeking to justify the Court's order based on those very same programs, arguing that they render Apple "intimately close" to the crime for purposes of the *New York Telephone* analysis. Opp. 16.

Second, the government does not dispute, or even discuss, that CALEA excludes "information services" providers from the scope of its mandatory assistance provisions. 47 U.S.C. § 1002(b)(2). Apple is indisputably an information services provider given the features of iOS, including Facetime, iMessage, and Mail. Opp. 14–16; Mot. 17 & n.23; 47 U.S.C. § 1001(6)(B)(i) (information services include "electronic messaging services" and services that "permit[] a customer to retrieve stored information from, or file information for storage in, information storage facilities"). And the "information services" provided by Apple are not limited to those specific person-to-person communications, but also include the system updates and status communications highlighted by the government. Opp. 14–15. CALEA therefore forbids requiring information services providers like Apple to configure their systems so as to give law enforcement access to its information services—in real-time or after such communications are stored on the device.

Finally, CALEA makes clear that even telecommunications carriers (a category of providers subject to more intrusive requirements under CALEA, but which Apple is not) cannot be required to "ensure the government's ability" to decrypt or to create decryption programs the company does not already "possess."[8] 47 U.S.C. § 1002(b)(3). If companies subject to CALEA's obligations cannot be required to bear this burden,

[8] Carriers "shall not be responsible for decrypting, *or ensuring the government's ability to decrypt*, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier *possesses the information necessary* to decrypt the communication." 47 U.S.C. § 1002(b)(3) (emphases added).

Congress surely did not intend to allow parties specifically exempted by CALEA (such as Apple) to be subjected to it. The government fails to address this truism.

CALEA's legislative history makes clear the sound policy reasons behind its specific limitations on when decryption services can be required. During congressional hearings on CALEA, then-FBI director Louis Freeh assured Senator Leahy that CALEA would not impede the growth of new technologies. When Senator Leahy asked whether CALEA would inhibit the growth of encryption, he responded "this legislation does not ask [companies] to decrypt. It just tells them to give us the bits as they have them. If they are [en]crypted, that is my problem." Ex. II at 4 [*Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375*, 103d Cong. 11 (1994)]. Congress thus considered shifting to third parties like Apple the very burden the government now asks this Court to impose, but it declined, knowing full well this meant there would be some communications that law enforcement could not access (and that developing the ability to access them would be "[the government's] problem," *see id*.). Neither the All Writs Act nor any case interpreting it allows the Court to issue an order that directly conflicts with this clear statutory prohibition. *See United States v. New York Tel. Co.*, 434 U.S. 159, 176 (1977) (relying on the fact that the proposed action was "consistent with . . . recent congressional actions").[9] Thus, even under the government's own (incorrect) view of the Act's authority, the relief the government seeks here is barred because Congress has prohibited it through a specific statute.

[9] The Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, specifically establishes when governmental entities can require providers of electronic communications and remote computing services to produce *stored* content to the government. The government can require such production when the content is "held or maintained on that service" or "in electronic storage" by the provider. *Id.* § 2703(a), (b). Neither prong applies to stored communications on the subject iPhone, as they are in the government's possession and not Apple's, and the SCA does not mandate decryption of communications that are not in Apple's possession.

2. Congress Refused To Grant The Power The Government Seeks.

The government wrongly asserts that legislative intent can never be discerned from an absence of affirmative legislation. Opp. 8–10. Although silence is sometimes a weak indicator of intent, it is a different story when Congress actively considers legislation to address a major policy issue, yet deliberately declines to enact it, *see, e.g.*, *Bob Jones Univ. v. United States*, 461 U.S. 574, 600 (1983) (Congress's "non-action" in the face of IRS opinions justified the inference that Congress agreed with those opinions), especially in the context of an elaborate and comprehensive statutory scheme, *P.R. Dep't of Consumer Affairs v. Isla Petroleum Corp.*, 485 U.S. 495, 503 (1988) ("Where a comprehensive federal scheme intentionally leaves a portion of the regulated field without controls, *then* preemptive inference can be drawn—not from federal inaction alone, but from inaction joined with action.").

Here, Congress chose to require limited third-party assistance in certain statutes designed to aid law enforcement in gathering electronic evidence (although none as expansive as what the government seeks here),[10] but it has declined to include similar provisions in other statutes, despite vigorous lobbying by law enforcement and notwithstanding its "prolonged and acute awareness of so important an issue" as the one presented here. *Bob Jones*, 461 U.S. at 601. Accordingly, the lack of statutory authorization in CALEA or any of the complementary statutes in the "comprehensive federal scheme" of surveillance and telecommunications law speaks volumes. *Isla Petroleum*, 485 U.S. at 503. To that end, Congress chose to "greatly narrow[]" the "scope of [CALEA]," which ran contrary to the FBI's interests but was "important from a privacy standpoint." H.R. Rep. No. 103-827(I), at 18 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3498. Indeed, CALEA's provisions were drafted to "limit[] the scope of [industry's] assistance requirements in several important ways." *Id.* at 23,

[10] In addition to CALEA, the Wiretap Act, 18 U.S.C. § 2518(4), the Pen/Trap Statute, *id.* § 3123(b)(2), the Electronic Communications Privacy Act ("ECPA"), *id.* § 2511(2)(a)(ii), and the SCA, *id.* § 2701, all specify circumstances in which a third party may be required to produce information to or assist law enforcement.

1994 U.S.C.C.A.N. at 3503. As the Ranking Member of the House Judiciary Committee recently put it:

> [F]or years . . . the Department of Justice and the [FBI] have urged this committee to give them the authority to mandate that companies create backdoors into their secure products[,] . . . [but] this committee, this Congress and the administration have so far refused to provide [that authority].

Ex. EE at 5 [Rep. Conyers, *Encryption Hr'g*].

That the Executive Branch recently abandoned plans to seek legislation expanding CALEA's reach (*see* Mot. 9) provides renewed confirmation that Congress has not acceded to the FBI's wishes, and belies the government's view that it has possessed such authority under the All Writs Act since 1789.[11]

Although the Administration is free to keep its powder dry for future lobbying efforts, the Constitution does not give the Executive Branch the "option" of asking the courts to rewrite CALEA. As demonstrated, CALEA's prohibition on the type of assistance the FBI seeks here is neither "hypothetical nor abstract" (Opp. 6), and this Court should decline the government's invitation to violate the separation of powers by usurping Congress's "exclusive constitutional authority to make laws." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 588–89 (1952).

The government's citation to *FTC v. Dean Foods Co.*, 384 U.S. 597 (1966), for the proposition that the Supreme Court has forbidden drawing meaning from

---

[11] The government's attempts to minimize CALEA II, saying its plans consisted of "mere[] vague discussions" that never developed into a formal legislative submission (Opp. 9), but federal officials familiar with that failed lobbying effort confirmed that the FBI had in fact developed a "draft proposal" containing a web of detailed provisions, including specific fines and compliance timelines, and had floated that proposal with the White House. *See* Dkt. 16-17 [Nakashima, *Proposal Seeks*]. As *The Washington Post* reported, advocates of the proposal within the government dropped the effort, because they determined they could not get what they wanted from Congress at that time: "Although 'the legislative environment is very hostile today,' the intelligence community's top lawyer, Robert S. Litt, said to colleagues in an August [2015] e-mail, which was obtained by The Post, 'it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement.' There is value, he said, in 'keeping our options open for such a situation.'" Ex. JJ [Ellen Nakashima & Andrea Peterson, *Obama Faces Growing Momentum to Support Widespread Encryption*, Wash. Post (Sept. 16, 2015)].

congressional silence in the All Writs Act context (Opp. 9), is simply inapposite. That case concerned the powers of the FTC, not the powers of the courts under the All Writs Act. 384 U.S. at 609. Also irrelevant is *United States v. Craft*, 535 U.S. 274 (2002), which the government invokes for the unremarkable proposition that, oftentimes, equally tenable conclusions can be drawn from failed legislation, including that Congress thought existing legislation already encompassed the proposed enactment. *See id.* at 287. Such an inference is not tenable here where Congress has faced sustained zealous lobbying, has actively debated granting the requested powers, and has made an affirmative decision not to do so. *Bob Jones*, 461 U.S. at 601. Rather, Congress has chosen to selectively provide and withhold authorizations in a "comprehensive federal scheme" of surveillance and telecommunications law, but has not granted the expansive authority the government seeks. *Isla Petroleum*, 485 U.S. at 503; *see also Trenkler v. United States*, 536 F.3d 85, 97 (1st Cir. 2008) (courts must "patrol . . . artful plead[ing]" about the "boundaries" of entitlements to writs in order to prevent "frustrat[ion] [of] Congress's discernible intent"); *Garland v. Sullivan*, 737 F.2d 1283, 1285–87 (3d Cir. 1984) (declining to construe the All Writs Act "as a grant of authority to transfer to the United States Treasury the expense of compliance with witness process" where the judiciary had no "statutory authorization"; "common sense and appropriate concern for separation of powers caution against such an arrogation of judicial power").

C. *New York Telephone* And Its Progeny Do Not Authorize The Order.

The conscription of a private company to write new software and create a new operating system that undermines the security of its own products—and thus the security and privacy of its users—cannot be equated with the "meager," not "offensive" assistance of a public utility allowed under *New York Telephone* and its progeny. 434 U.S. at 174.

1. Apple Is Far Removed From This Matter.

Apple's connection to this case is too attenuated to support an order compelling it to create new software that provides a back door to the iPhone. Whereas the public utility in *New York Telephone* was not "so far removed" from the matter because its facilities were "being employed to facilitate a criminal enterprise on a continuing basis," and the assistance requested involved setting up a routine pen register on a phone line that the utility owned and operated, 434 U.S. at 174, Apple is a private company that does not own or possess the phone at issue, has no existing means of accessing the data that may or may not exist on the phone, and is not related to the underlying criminal activity, which is not ongoing but ceased months ago.

The government argues that "courts have already issued AWA orders" requiring manufacturers to "unlock" phones (Opp. 13 (citing cases)), but those cases involved orders requiring "unlocking" assistance to provide access through existing means, not the extraordinary remedy sought here, *i.e.*, an order that requires creating new software to undermine the phones' (or in the *Blake* case, the iPad's) security safeguards. The orders in those cases were also issued *ex parte* without the benefit of adversarial briefing and without confronting *New York Telephone*'s "far removed" analysis.

The government discusses Apple's software licensing and data policies at length, equating Apple to a feudal lord demanding fealty from its customers ("suzerainty"). Opp. 14–16. But the government does not cite *any* authority, and none exists, suggesting that the design features and software that exist on *every* iPhone somehow link Apple to the subject phone and the crime. Likewise, the government has cited no case holding that a license to use a product constituted a sufficient connection under *New York Telephone*. Indeed, under the government's theory, any ongoing post-purchase connection between a manufacturer or service provider and a consumer suffices to connect the two in perpetuity—even where, as here, the data on the iPhone is inaccessible to Apple.

Finally, each of the government's authorities involved minimal assistance by a third party in thwarting an *ongoing* crime that was (1) being facilitated by the third parties' products (*United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (ordering bank to produce credit card records, where card was potentially being used to support fugitive)); (2) occurring on the third parties' premises (*In re Application of the U.S. for an Order Directing X to Provide Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (ordering apartment complex to provide access to *existing* surveillance footage where government had reason to suspect that fugitive would return to the complex)); or (3) using the third parties' facilities (*In re Application of the U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities (Mountain Bell)*, 616 F.2d 1122, 1132–33 (9th Cir. 1980) (ordering public utility to assist in setting up pen trap where the utilities' facilities were suspected of being used for ongoing crime)). The government also relies on a case in which the court compelled a *defendant*—not a third party—to provide the "unencrypted contents" of her computer (Opp. 14 (citing *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012)), but that case has no bearing on the remoteness of a *third party's* connection to a case.

2. The Order Would Impose Unprecedented And Offensive Burdens.

Forcing Apple to create new software that degrades its security features is unprecedented and unlike any burden ever imposed under the All Writs Act. The government's assertion that the phone companies in *Mountain Bell* and *In re Application of the U.S. for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and a Terminating Trap (Penn Bell)*, 610 F.2d 1148 (3d. Cir. 1979), were conscripted to "write" code, akin to the request here (Opp. 18–19), mischaracterizes the actual assistance required in those cases. The government seizes on the word "programmed" in those cases and superficially equates it to the process of creating new software. Opp. 18–19. But the "programming" in those cases—back in 1979 and 1980—consisted of a "technician" using a "teletypewriter" in *Mountain Bell* (Dkt. 149-1 [Wilkison Decl.] Ex. 6 at 7), and "t[ook] less than one minute" in *Penn Bell*

(610 F.2d at 1152–53). Indeed, in *Mountain Bell*, the government itself stated that the only burden imposed "was a large number of print-outs on the teletype machine"—not creating new code. Ex. KK at 23–24 [Gov't Br.]. More importantly, the phone companies *already had* and *themselves used* the tracing capabilities the government wanted to access. *See Mountain Bell*, 616 F.2d at 1126; *Penn Bell*, 610 F.2d at 1152–54 (*e.g.*, to "locate[] defect[s]" and to help customers, "free of charge," to identify "annoying call[ers]").[12] And although relying heavily on *Mountain Bell*, the government neglects to point out the court's explicit warning that "[t]his holding is a narrow one, and our decision today should not be read to authorize the wholesale imposition upon private, third parties of duties pursuant to search warrants." 616 F.2d at 1132.[13] This case stands light years from *Mountain Bell*. The government seeks to commandeer Apple to design, create, test, and validate a new operating system that does not exist, and that Apple believes—with overwhelming support from the technology community and security experts—is too dangerous to create.[14]

Seeking to belittle this widely accepted policy position, the government grossly mischaracterizes Apple's objection to the requested Order as a concern that "compliance will tarnish its brand" (Opp. 22), a mischaracterization that both the FBI Director and the courts have flatly rejected. *See* Ex. EE at 15 [Comey, *Encryption Hr'g*] ("I don't

---

[12] The government's reliance on *Gonzalez v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (Opp. 19 n.7), is also misplaced, because it is not an All Writs Act case and analyzes the burden imposed under a completely different framework for civil discovery. Also, the government fails to mention that in *Gonzalez*, Google could "extract the information requested from its existing systems," 234 F.R.D. at 683, unlike this case, where Apple would be required to create an entirely new operating system.

[13] The government's desire to "develop all relevant facts" (Opp. 17 (internal quotation marks omitted)), while understandable, is not, and never has been, a sufficient justification for invoking the All Writs Act. *See Ivey*, 47 F.3d at 184–186 (refusing relief even though plaintiff may have "no hope of prevailing in the underlying litigation").

[14] The government also implicitly threatens that if Apple does not acquiesce, the government will seek to compel Apple to turn over its source code and private electronic signature. Opp. 22 n.9. The catastrophic security implications of that threat only highlight the government's fundamental misunderstanding or reckless disregard of the technology at issue and the security risks implicated by its suggestion.

question [Apple's] motive"); *In re Apple, Inc.*, 2016 WL 783565, at *21 n.35 (disagreeing "with the government's contention that Apple's objection [to being compelled to decrypt an iPhone] is not 'conscientious' but merely a matter of 'its concern with public relations'").[15] As Apple explained in its Motion, Apple prioritizes the security and privacy of its users, and that priority is reflected in Apple's increasingly secure operating systems, in which Apple has chosen *not* to create a back door.[16] Compelling Apple to reverse that choice is "offensive to it." *New York Tel. Co.*, 434 U.S. at 174. The government attempts to dilute *New York Telephone* by making the obvious and irrelevant point that "programming software is not 'offensive' to Apple generally." Opp. 23. But the Court was not concerned with whether the phone company considered operating pen registers to be "generally" offensive—of course it was not, because the company "regularly employ[ed] such devices." 434 U.S. at 174. The Court instead, in the context of weighing the privacy interests implicated by the use of pen registers, was concerned with whether the company found it "offensive" in the specific context of the government's request—finding that it was not, given the company's own similar use, "without court order," to "detect[] fraud" and "prevent[] violations of law," and that the company had earlier "agreed to supply the FBI with all the information required to install its own pen registers." *Id*. at 174–75. By contrast, Apple has never built, and would find it "offensive" to build GovtOS.

[15] The government accuses Apple of developing the passcode-based encryption features at issue in this case for marketing purposes. *E.g.*, Opp. 1, 22. This is a reckless and unfounded allegation. Since passcode-based encryption was first introduced in October 2014, Apple has produced 627 separate ads in the United States and approximately 1,793 ads worldwide. Ferrini Declaration ¶ 5. These ads have generated 99 and 253 billion impressions, respectively. *Id.* Not a single one advertised or promoted the ability of Apple's software to block law enforcement requests for access to the contents of Apple devices. *Id.* ¶ 6.

[16] The idea that Apple enhances its security to confound law enforcement is nonsense. Apple's "chain of trust" process—which follows accepted industry best practices—is designed to secure its mobile platform against the never-ending threat from hackers and cyber-criminals. *See* Neuenschwander Supp. Decl. ¶¶ 4–15. It is the same process that helps protect desktop computers from viruses and Trojan horses, and that ensures hackers do not tamper with the software on automobiles. *Id.* ¶¶ 14–15.

Moreover, there is no question the back door, if built, will be used repeatedly and poses grave security risks. The government contends that there is "no precedent for considering possible prospective burdens as a basis for withholding a narrow AWA order now." Opp. 27. But in *Plum Creek*, the Ninth Circuit declined to issue an AWA order in part because of the prospective risks and costs that would be imposed on the company by OSHA's request to compel it to use certain equipment to aid OSHA's investigation of the company's premises. 608 F.2d at 1289 & n.4. Similarly, in assessing the burden imposed by the tracing order in *Mountain Bell*, the Ninth Circuit considered the risk of system malfunction caused by that trace "*in conjunction with other court-ordered traces*." 616 F.2d at 1132 (emphasis added). Here, if Apple is forced to create software in this case, other law enforcement agencies will seek similar orders to help them hack thousands of other phones, as FBI Director Comey confirmed when he said he would "of course" use the All Writs Act to "return to the courts in future cases to demand that Apple and other private companies assist . . . in unlocking secure devices." Ex. EE at 15 [*Encryption Hr'g*].[17] Meanwhile, "[e]ncryption[] [will] always be[] available to bad actors," as Director Comey conceded, *id*. at 23–24, creating a perverse unilateral disarmament through the erosion of the strong defense against cyberterrorism. *See* Ex. LL at 20 [*Encryption Hr'g*] (Prof. Landau, stating the requested

[17] *See also* Ex. LL at 10 [*Encryption Hr'g*] (Vance: "thousands of phones"); Ex. EE at 22 [*Encryption Hr'g*] (Rep. Nadler: "[W]e all understand that it's not just a specific case."); Dkt. 70 [Fed. Law Enforcement Officers' Assoc. *amicus* brief] at 6–9 (noting requests for similar orders will follow, in cases ranging from homicide to identity theft). Indeed, Richard Clarke, former National Coordinator for Security, Infrastructure Protection and Counter-terrorism, recently stated his belief that the FBI is "not as interested in solving the problem as they are in getting a legal precedent . . . that the government can compel a computer device manufacturer to allow the government in." Ex. MM [*Encryption, Privacy Are Larger Issues Than Fighting Terrorism, Clarke Says*, NPR (Mar. 14, 2016)]; *see also* Ex. NN [Yoni Heisler, *Former CIA Director Calls out the FBI for Wanting to Fundamentally Change the iPhone*, BGR (Mar. 11, 1016)] (Former CIA Director James Woolsey: "[I]t did seem to me as if the FBI was trying to get a right essentially to effectively decide what kind of an operating system Apple was going to have, and that they were not just trying to get into one phone.").

Order "would weaken us but not change [the availability of strong encryption] for the bad guys").

The government's assertion that "there is no reason to think that the code Apple writes in compliance with the Order will ever leave Apple's possession" (Opp. 24), simply shows the government misunderstands the technology and the nature of the cyber-threat landscape. As Apple engineer Erik Neuenschwander states:

> I believe that Apple's iOS platform is the most-attacked software platform in existence. Each time Apple closes one vulnerability, attackers work to find another. This is a constant and never-ending battle. Mr. Perino's description of third-party efforts to circumvent Apple's security demonstrates this point. And the protections that the government now asks Apple to compromise are the most security-critical software component of the iPhone—any vulnerability or back door, whether introduced intentionally or unintentionally, can represent a risk to all users of Apple devices simultaneously.

Neuenschwander Supp. Decl. ¶ 28. The government is also mistaken in claiming that the crippled iOS it wants Apple to build can only be used on one iPhone:

> Mr. Perino's characterization of Apple's process . . . is inaccurate. Apple does not create hundreds of millions of operating systems each tailored to an individual device. Each time Apple releases a new operating system, that operating system is the same for every device of a given model. The operating system then gets a personalized signature specific to each device. This personalization occurs as part of the installation process after the iOS is created.
>
> Once GovtOS is created, personalizing it to a new device becomes a simple process. If Apple were forced to create GovtOS for installation on the device at issue in this case, it would likely take only minutes for Apple, or a malicious actor with sufficient access, to perform the necessary engineering work to install it on another device of the same model.
>
> . . . [T]he initial creation of GovtOS itself creates serious ongoing burdens and risks. This includes the risk that if the ability to install GovtOS got into the wrong hands, it would open a significant new avenue of attack, undermining the security protections that Apple has spent years developing to protect its customers.

Id. ¶¶ 17–19.

Cybersecurity experts agree. *E.g.*, Ex. OO [*Experts: The FBI's iPhone-Unlocking Plan for Apple Is Risky*, Chi. Trib. (Feb. 22, 2016)] ("[I]t may simply be impossible to keep the program from falling into the wrong hands."); Ex. OO (quoting former NSA expert Will Ackerly: "[u]sing the software even once could give authorities or outsiders new clues to how Apple's security features work, potentially exposing vulnerabilities

that could be exploited in the future"); Ex EE at 5 [Rep. Conyers, *Encryption Hr'g*] ("The technical experts have warned us that it is impossible to intentionally introduce flaws into secure products—often called backdoors—that only law enforcement can exploit to the exclusion of terrorists and cyber criminals."); Dkt. 82 [Experts' *amicus* brief] at 10 (the government's proposed safeguards "are not meaningful barriers to misuse and abuse of the forensic capabilities this Court is ordering Apple to create"); *id.* at 18 ("A signed firmware update that is not truly limited to a single device, even one created for legitimate forensic purposes, becomes like a 'skeleton key' for the entire class of devices.").[18] Moreover, the more often this tool is used, the greater the risk it will be stolen or otherwise disclosed. Ex. RR at 17 [Prof. Landau, Written Testimony *Encryption Hr'g*] ("routinization will make it too easy for a sophisticated enemy"); *see* Neuenschwander Supp. Decl. ¶ 20. No All Writs Act authority permits courts to require an innocent private company to create and maintain code whose "public danger is apparent" and whose disclosure would be "catastrophic" to the security and privacy interests of hundreds of millions of users.[19] Dkt. 82 [Experts' *amicus* brief] at 15.

Finally, the government attempts to disclaim the obvious international implications of its demand, asserting that any pressure to hand over the same software to foreign agents "flows from [Apple's] decision to do business in foreign countries . . . ." Opp. 26. Contrary to the government's misleading statistics (Opp. 26), which had to do

---

[18] *See also* Ex. PP [Kalev Leetaru, *Why the Apple Versus FBI Debate Matters in a Globalized World*, Forbes (Mar. 2, 2016)] ("[T]here is no way to make a backdoor that works only for this single phone—the process of creating the backdoor establishes a blueprint and workflow for compromising all iPhones."); Ex QQ [Elizabeth Weise, *Chertoff: iPhone Override Is Software Equivalent of Biological Weapon*, USA Today (Mar. 4, 2016) ("Once you've created code that's potentially compromising, it's like a bacteriological weapon. You're always afraid of it getting out of the lab.").

[19] Even Apple devices are not immune from cyberattack. Ex. SS [Jim Finkle, *Mac Ransomware Caught Before Large Number of Computers Infected*, Reuters (Mar. 7, 2016)] (describing attack on Mac computers in which hackers successfully installed malicious software by uploading disguised malicious software to a third party site and using a public digital certificate—a cryptographic signature—to trick the computers into believing the malicious code was trustworthy).

with *lawful* process and did not compel the creation of software that undermines the security of its users, Apple has *never* built a back door of any kind into iOS, or otherwise made data stored on the iPhone or in iCloud more technically accessible to any country's government. *See* Dkt. 16-28 [Apple Inc., *Privacy, Gov't Info. Requests*]; Federighi Decl. ¶¶ 6–7. The government is wrong in asserting that Apple made "special accommodations" for China (Opp. 26), as Apple uses the same security protocols everywhere in the world and follows the same standards for responding to law enforcement requests. *See* Federighi Decl. ¶ 5.

3. The Government Has Not Demonstrated Necessity.

The government does not deny that there may be other agencies in the government that could assist it in unlocking the phone and accessing its data; rather, it claims, without support, that it has no obligation to consult other agencies. Opp. 30; *see also* Ex. MM [*Encryption, Privacy Are Larger Issues Than Fighting Terrorism, Clarke Says*, NPR (Mar. 14, 2016)] (quoting Richard Clarke (former National Coordinator for Security, Infrastructure Protection and Counter-terrorism): "Every expert I know believes that NSA could crack this phone."); Ex. RR at 13 [Prof. Landau, Written Testimony, *Encryption Hr'g*] (noting that "solutions to accessing the data *already exist within the forensic analysis community*"); Ex EE at 26–28 [*Encryption Hr'g*] (Rep. Issa asking Director Comey a series of questions as to the avenues the FBI exhausted, to which the Director said he did not know, and Rep. Issa replying, "If you haven't asked that question, the question is how can you come before this committee, and before a federal judge, and demand that somebody else invent something[?]").[20] Indeed, if nothing else, the Perino Declaration demonstrates that the government and "third parties

[20] Defining the scope of the All Writs Act as inversely proportional to the capabilities of the FBI removes any incentive for it to innovate and develop more robust forensic capabilities. *See* Ex. LL at 7–8 [Prof. Landau, *Encryption Hr'g*] ("The FBI needs to take a page from the NSA. You may recall that in the late 1990s, the NSA was complaining it was going deaf from encrypted calls? Well, they've obviously improved their technology a great deal. . . . Rather than asking industry to weaken protections, law enforcement must instead develop a capability for conducting sophisticated investigations themselves.").

have already come close to developing a tool that would defeat part of iOS's present security capabilities." Neuenschwander Supp. Decl. ¶ 29. Moreover, while they now argue that the FBI's changing of the iCloud passcode—which ended any hope of backing up the phone's data and accessing it via iCloud—"was the reasoned decision of experienced FBI agents" (Opp. 29), the FBI Director himself admitted to Congress under oath that the decision was a "mistake" (Ex. EE at 22 [*Encryption Hr'g*]). The Justice Department's shifting, contradictory positions on this issue—first blaming the passcode change on the County, then admitting that the FBI told the County to change the passcode after the County objected to being blamed for doing so, and now trying to justify the decision in the face of Director Comey's admission that it was a mistake (*id.*)—discredits any notion that the government properly exhausted all viable investigative alternatives before seeking this extraordinary order from this Court. *See New York Tel. Co.*, 434 U.S. at 175 (noting there "there [wa]s no conceivable way" for the government to obtain the pen register data). Finally, the government's showing of need for this unprecedented order is speculative at best. Ex. TT [*San Bernardino Police Chief Sees Chance Nothing of Value on Shooter's iPhone*, NPR (last updated Mar. 2, 2016)] ("I'll be honest with you, I think that there is a reasonably good chance that there is nothing of any value on the phone.").

D. The Order Would Violate The First Amendment And Due Process Clause.

The government begins its First Amendment analysis by suggesting that "[t]here is reason to doubt that functional programming is even entitled to traditional speech protections" (Opp. 32), evincing its confusion over the technology it demands Apple create.[21] Even assuming there is such a thing as *purely* functional code, creating the type of software demanded here, an operating system that has never existed before, would necessarily involve precisely the kind of expression of ideas and concepts protected by

[21] The government also wrongly suggests that Apple can simply leverage existing hacking software to accomplish the government's demands. Using third-party software would cause more problems than it would solve. *See* Neuenschwander Supp. Decl. ¶¶ 21-26.

the First Amendment. Because writing code requires a choice of (1) language, (2) audience, and (3) syntax and vocabulary, as well as the creation of (4) data structures, (5) algorithms to manipulate and transform data, (6) detailed textual descriptions explaining what code is doing, and (7) methods of communicating information to the user, "[t]here are a number of ways to write code to accomplish a given task." Dkt. 16-33 [Neuenschwander Decl.], ¶¶ 65–66; *see also* Ex. UU [Jonathan Keats, *Code Isn't Just Functional, It's Poetic*, Wired (Apr. 16, 2013)]. As such, code falls squarely within the First Amendment's protection, as even the cases cited by the government acknowledge.[22] *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449–50 (2d Cir. 2001) ("[C]omputer code conveying information is 'speech' within the meaning of the First Amendment."); *United States v. Elcom, Ltd.*, 203 F. Supp. 2d 1111, 1127 (N.D. Cal. 2002) ("'[C]omputer code is covered, or as sometimes said, "protected" by the First Amendment.'" (quoting *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 327 (S.D.N.Y. 2000))).

The government next insists that it seeks only to "compel[] conduct—namely, the removal of barriers from Farook's iPhone—with an incidental effect on 'speech.'" Opp. 33. But the government has it exactly backwards—it is asking the Court to compel Apple to engage in speech, writing code that is "offensive to it," *New York Tel. Co.*, 434 U.S. at 174, and that it vigorously opposes—to help the government engage in the conduct of "brute-forcing" the iPhone to try to determine the passcode. As the Supreme Court observed in *Riley v. National Federation of the Blind of North Carolina, Inc.*, "[m]andating speech that a speaker would not otherwise make necessarily alters the content of the speech[,]" and laws imposing such mandates should be "consider[ed] . . .

[22] Although the government suggests that the code it requests is not speech because "there is no audience" (Opp. 33), this has never been a requirement for First Amendment protection. *See Spence v. Washington*, 418 U.S. 405, 409 (1974) (per curiam) (holding that the display of an upside-down American flag was speech "[a]lthough the stipulated facts fail to show that any member of the general public viewed the flag," as the display had a communicative element).

content-based regulation[s] of speech." 487 U.S. 781, 795 (1988) (applying strict scrutiny).

The government attempts to evade this unavoidable conclusion by insisting that, "[t]o the extent [that] Apple's software includes expressive elements . . . the Order permits Apple to express whatever it wants, so long as the software functions" by allowing it to hack into iPhones. Opp. 32–33. This serves only to illuminate the broader speech implications of the government's request. The code that the government is asking the Court to force Apple to write contains an extra layer of expression unique to this case. When Apple designed iOS 8, it consciously took a position on an issue of public importance. *See, e.g.*, Dkt. 16-28 [Apple Inc., *Privacy Policy*] ("We believe security shouldn't come at the expense of individual privacy."). The government disagrees with Apple's position and asks this Court to compel Apple to write new code that reflects its own viewpoint—a viewpoint that is deeply offensive to Apple. *Cf. New York Tel. Co.,* 434 U.S. at 174 (observing that "the use of pen registers is by no means offensive" to the objecting party).

The closest case the government can find to support its unprecedented intrusion on free speech is *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47 (2006), which held that Congress has the power under the Spending Clause to make federal funding for law schools conditional on those schools granting access to military recruiters on equal terms as others. This is a stretch to say the least.

There is an obvious difference between a recruitment event at a law school—which would likely constitute a limited public forum at state-funded schools, *see Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 829 (1995)—and forcing Apple to write new and unwanted code. Indeed, Apple is not only being asked to *design* this code, but to cryptographically *sign* it, thereby endorsing code that it deems dangerous. *See* Dkt. 16-33 [Neuenschwander Decl.], ¶¶ 18, 27-28.

The government's position has sweeping implications. Under the government's view, the state could force an artist to paint a poster, a singer to perform a song, or an

author to write a book, so long as its purpose was to achieve some permissible end, whether increasing military enrollment or promoting public health. "Accepting the Government's theory would give [it] the [] license to regulate what we do *not* do, fundamentally changing the relation between the citizen and the Federal Government." *Nat'l Fed'n of Indep. Bus. v. Sebelius*, 132 S. Ct. 2566, 2589 (2012) (opinion of Roberts, C.J.) (emphasis added). The First Amendment does not permit such a wholesale derogation of Americans' right not to speak.

Finally, the government knows Apple does not espouse some *Lochner*-era theory of unfettered economic right to marketing activity. *See* Opp. 35. It knows that Apple instead objects to the government's attempted conscription of it to send individual citizens into a super-secure facility to write code for several weeks on behalf of the government on a mission that is contrary to the values of the company and these individuals. Such conscription is fundamentally "offensive to" Apple's core principles, and would "pose a severe threat to the autonomy" of Apple and its engineers. *New York Tel. Co.*, 434 U.S. at 171, 174. That violates due process. *Cf. Obergefell v. Hodges*, 135 S. Ct. 2584, 2597 (2015) (due process protects "personal choices central to individual . . . autonomy").

III. CONCLUSION

Almost 90 years ago, Justice Louis Brandeis, reflecting on the "progress of science" beyond wiretapping, famously warned that "[t]he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." *Olmstead v. United States*, 277 U.S. 438, 474, 479 (1928). In this case, the government's motivations are understandable, but its methods for achieving its objectives are contrary to the rule of law, the democratic process, and the rights of the American people. The Court should vacate the order and deny the government's motion to compel.

Dated: March 15, 2016

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: /s/ Theodore J. Boutrous Jr.

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

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

Marc J. Zwillinger *
Jeffrey G. Landis *
ZwillGen PLLC
1900 M Street N.W., Suite 250
Washington, DC 20036
Telephone: 202.706.5202
Facsimile: 202.706.5298
*Admitted Pro Hac Vice

Attorneys for Apple Inc.